AIRPORTS
WORLDWIDE

TABLE OF CONTENTS

INTRODUCTION

This Code of Ethics is designed to deter wrongdoing and to promote:

- honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- compliance with applicable laws, rules and regulations;
- the prompt internal reporting of violations of this Code; and
- accountability for adherence to this Code.

This Code applies to all directors, officers, and employees of the company and its affiliates, who, unless otherwise specified, will be referred to jointly as employees. Members of a company consortium, agents, consultants, service providers and other independent contractors of the company are also expected to read, understand, and abide by this Code to the extent applicable. Specifically relating to members of a company consortium, and companies that are shareholders in companies or ventures wherein Airports Worldwide has a financial and/or legal interest, Airports Worldwide recognizes that some of the specific procedures for compliance, and reporting structures, described in the Code may not be applicable. Nevertheless, such members or companies must comply with the FCPA and all other applicable anti-corruption laws and it is the expectation of Airports Worldwide that such members or companies disclose and demonstrate their own internal procedures, policies, and practices for full compliance with same and the principles described in this Code.

The term "company" as used in this Code refers to Airports Worldwide, Inc., a Texas Corporation. The term "affiliate" means, with respect to the company, any individual or entity directly or indirectly controlling, controlled by or under common control with, the company. For the purposes of this definition, "control" (including, with correlative meaning, the terms "controlling," "controlled by" and "under common control with") shall mean the possession, directly or indirectly, of the power to direct or cause the direction of management and policies of the individual or entity, whether through the ownership of voting securities, by contract or otherwise. The term "company consortium" shall include any consortium, bidding cooperative or similar association in which the company or any affiliate is a member.

This Code should help guide your conduct in the course of our business. However, many of the principles described in this Code are general in nature, and the Code does not cover every situation that may arise. Use common sense and good judgment in applying this Code. If you have any questions about applying the Code, it is your responsibility to seek guidance.

This Code is not the exclusive source of guidance and information regarding the conduct of our business. You should consult applicable policies and procedures in specific areas as they apply. The Code is intended to supplement, not replace, the employee policies and procedures of the company.

We are committed to continuously reviewing and updating our policies and procedures. The company therefore reserves the right to amend, alter or terminate this Code at any time and for any reason, subject to applicable law.

YOUR RESPONSIBILITIES

• You are expected to read and understand this Code.

• You must uphold these standards in day-to-day activities and comply with all applicable policies and procedures in the Code.

• Regardless of the relationship you maintain with the company and/or its affiliates, your duties and ethical responsibility are to help enforce this Code. You should be alert to possible violations and promptly report violations or suspected violations of this Code to the Compliance Manager of Airports Worldwide, Inc.. If you wish to remain anonymous, send a letter addressed to Airports Worldwide, Inc., attention: the Compliance Manager, at 15600 JFK Blvd., Suite 110, Houston, Texas USA 77032. If you make an anonymous report, please provide as much detail as possible, including copies of any documents that you believe may be relevant to the issue.

• If your concerns relate to accounting, internal controls or auditing matters, you may contact the CFO of Airports Worldwide, Inc., at 15600 JFK Blvd., Suite 110, Houston, Texas USA 77032. If the Compliance Manager is implicated in any violation or suspected violation, you may also contact the HR Manager, at 15600 JFK Blvd., Suite 110, Houston, Texas USA 77032. You must cooperate with investigations into possible Code violations and be truthful and forthcoming in the course of these investigations.

• Reprisals, threats, retribution or retaliation against any person who has in good faith reported a violation or a suspected violation of law, this Code or other company policies, or against any person who is assisting in good faith in any investigation or process with respect to such a violation, is prohibited.

• In trying to determine whether any given action is appropriate, keep these steps in mind:

- ✓ Obtain all relevant facts.
- ✓ Assess the responsibilities and roles of those involved.
- ✓ Using your judgment and common sense, evaluate whether the action seems unethical or improper.
- ✓ Seek guidance.

• If you are unsure about any situation or any provision of the Code, discuss the matter with your immediate supervisor or the Compliance Manager of Airports Worldwide, Inc.

GENERAL STANDARDS OF CONDUCT

Overview

Honest and ethical conduct is critical to our business. All employees, agents, and contractors have a duty to comply with applicable law and to act in an honest and ethical manner.

Compliance with Law

You are responsible for complying with all laws, rules, regulations and regulatory orders applicable to the conduct of our business. If you are located or engaging in business outside of the United States, you must comply with laws, rules, regulations and regulatory orders of the United States, including the Foreign Corrupt Practices Act (referred to in this Code as the "FCPA") and U.S. export rules and regulations, in addition to the applicable laws of other jurisdictions, including the UK Bribery Act 2010 (“UK Bribery Act”). If compliance with the Code should ever conflict with law, you must comply with the law.

You should take efforts to learn the legal requirements relating to your duties so you can recognize potential dangers and know when to seek advice from managers, supervisors, Human Resources, the Compliance Manager, or other appropriate personnel.

Violations of laws, rules, regulations and orders may subject you to individual civil or criminal liability, which may include fines or imprisonment, in addition to discipline by the company.

No Discrimination or Harassment

The company is committed to providing a work environment that is free of discrimination and harassment. The company (and each affiliate of the company) is an equal opportunity employer and makes employment decisions on the basis of merit and business needs. The company (and each affiliate of the company) strictly prohibits harassment of any kind, including harassment on the basis of race, ancestry, veteran status, religion, gender, sex, sexual orientation, age, mental or physical disability, medical condition, family care status, national origin, marital status or any other characteristics protected under federal or state law or local ordinance.

Health and Safety

You are responsible for using good judgment to help ensure a safe and healthy workplace for all employees.

AVOIDING CONFLICTS OF INTERESTS

Overview

Your decisions and actions in the course of your employment or relationship with the company or an affiliate should be based on the best interest of the company and the particular affiliate, and not based on personal relationships or benefits. You should seek to avoid situations where your personal activities and relationships conflict, or appear to conflict, with the interests of the company or any affiliate, except under guidelines approved by the company. This includes situations where you may have or appear to have an indirect conflict through, for example, a significant other or a relative or other persons or entities with which you have a relationship. A conflict may also arise when you take actions or have interests that make it difficult for you to perform your work for the company or an affiliate of the company objectively and effectively. You must disclose to your manager any interest that you have that may, or may appear to, conflict with the interests of the company or any affiliate.

There are a variety of situations in which a conflict of interest may arise. While it would be impractical to attempt to list all possible situations, some common types of conflicts are discussed below.

Outside Employment and Directorships

Unless you are a non-employee director, you may not perform services as a director, employee, agent or contractor for a customer, other members of a company consortium, contractors, vendors, partners, or any other entity that has a business relationship with the company or an affiliate without approval from the company. Non-employee directors must promptly inform the company of any such service. You may not perform services as a director, employee, agent or contractor of any competitor of the company or its affiliates.

Financial Interests in Other Companies

You should not have a financial interest—including an indirect interest through, for example, a relative or significant other—in any organization if that interest would give you or would appear to give you a conflict of interest with the company or its affiliates. You should be particularly sensitive to financial interests in competitors, customers, members of a company consortium, contractors or vendors.

Transactions with Related Parties

If you have a significant financial interest in a transaction between the company or an affiliate, on the one hand, and a third party, on the other hand—including an indirect interest through, for example, a relative or significant other—you must disclose that interest, and that interest must be approved by the company. We encourage you to seek guidance if you have any questions as to whether an interest in a transaction is significant. Any dealings with a related party must be conducted in such a way that no preferential treatment is given to this business.

Corporate Opportunities

You may not directly or indirectly exploit for personal gain any opportunities that are discovered through the use of property of the company or an affiliate, information or position unless the opportunity is disclosed fully in writing to the company and the company declines to pursue the opportunity.

Loans by the Company

Loans from the company or any affiliate to directors and executive officers are prohibited, unless approved by the company or the affiliate. Loans from the company or any affiliate to other officers and employees must be approved in advance by the company or the affiliate.

Improper Benefits

You may not receive any improper benefit as a result of your position or relationship with the company or any affiliate.

Election or Appointment to Public Office

You may serve in an elected or appointed public office provided that the position does not create or appear to create a conflict of interest.

Guidance and Approvals

Evaluating whether a conflict of interest exists, or may appear to exist, requires the consideration of many factors. We encourage you to seek guidance and approval in any case where you have any questions or doubts. The company may at any time rescind prior approvals to avoid a conflict of interest, or the appearance of a conflict of interest, for any reason deemed to be in the best interest of the company or its affiliates.

COMMUNICATIONS

Communications and Filings

The company and its affiliates from time to time prepare and file reports and other documents with regulatory authorities. In addition, the company and its affiliates may make other public communications, such as issuing press releases.

Depending upon your position or relationship with the company or its affiliates, you may be called upon to provide information to help assure that such reports and communications are complete, fair, accurate and understandable. You are expected to use all reasonable efforts to provide complete, accurate, objective, relevant, timely and understandable answers to inquiries related to such reports and communications.

Individuals involved in the preparation of reports and communications must use all reasonable efforts to ensure full, fair, accurate, timely and understandable disclosure in our reports and communications.

If you believe that any disclosure is materially misleading or if you become aware of any material information that you believe should be disclosed to the public, it is your responsibility to bring this information to the attention of the company, attention: the Compliance Manager, of Airports Worldwide, Inc., at 15600 JFK Blvd., Suite 110, Houston, Texas USA 77032. If you believe that questionable accounting or auditing conduct or practices have occurred or are occurring, you should notify the company, attention: the Chief Financial Officer of Airports Worldwide, Inc., at 15600 JFK Blvd., Suite 110, Houston, Texas USA 77032.

Communication Procedures

You may not communicate externally on behalf of the company or any of its affiliates unless you are authorized to do so. The company has established specific policies regarding who may communicate information to the public, the press, market professionals (such as securities analysts, institutional investors, investment advisors, brokers and dealers) and security holders. Our Chief Executive Officer and his authorized designees, are our official spokespeople for financial matters, public comment, press, marketing, technical and other such information.

You should refer all calls or other inquiries from the press, market professionals or security holders to the Chief Executive Officer of the company, which will see that the inquiry is directed to the appropriate persons within the company.

FINANCIAL REPORTING

Overview

We are required to follow strict accounting principles and standards, to report financial information accurately and completely in accordance with these principles and standards, and to have appropriate internal controls and procedures to ensure that our accounting and financial reporting complies with law. The integrity of our financial transactions and records is critical to the operation of our business and is a key factor in maintaining the confidence and trust of our employees, security holders and other stakeholders.

Compliance with Rules, Controls and Procedures

It is important that all transactions are properly recorded, classified and summarized in our financial statements, books and records in accordance with our policies, controls and procedures, as well as all generally accepted accounting principles, standards, laws, rules and regulations for accounting and financial reporting. If you have responsibility for or any involvement in financial reporting or accounting, you should have an appropriate understanding of, and you should seek in good faith to adhere to, relevant accounting and financial reporting principles, standards, laws, rules and regulations and the company's financial and accounting policies, controls and procedures. If you are a senior officer, you should seek to ensure that the internal controls and procedures in your business area are in place, understood and followed.

Accuracy of Records and Reports

It is important that those who rely on records and reports—managers and other decision makers, creditors, customers and auditors—have complete, accurate and timely information. False, misleading or incomplete information undermines the company's ability to make good decisions about resources, employees and programs and may in some cases result in violations of law. Anyone involved in preparing financial or accounting records or reports, including financial statements and schedules, must be diligent in assuring that those records and reports are complete, accurate and timely. Anyone representing or certifying as to the accuracy of such records and reports should make an inquiry or review adequate to establish a good faith belief in their accuracy.

Even if you are not directly involved in financial reporting or accounting, you are likely involved with financial records or reports of some kind—a voucher, time sheet, invoice or expense report. In addition, most employees have involvement with product, marketing or administrative activities, or performance evaluations, which can affect our reported financial condition or results. Therefore, the company expects you, regardless of whether you are otherwise required to be familiar with finance or accounting matters, to use all reasonable efforts to ensure that every business record or report with which you deal is accurate, complete and reliable.

Intentional Misconduct

You may not intentionally misrepresent the financial performance of the company or its affiliates or otherwise intentionally compromise the integrity of reports, records, policies and procedures. For example, you may not:

- report information or enter information in the books, records or reports of the company or its affiliates that fraudulently or intentionally hides, misrepresents or disguises the true nature of any financial or non-financial transaction or result;

- establish any undisclosed or unrecorded fund, account, asset or liability for any improper purpose;

- enter into any transaction or agreement that accelerates, postpones or otherwise manipulates the accurate and timely recording of revenues or expenses;

- intentionally misclassify transactions as to accounts, business units or accounting periods; or

- knowingly assist others in any of the above.

Dealing with Auditors

Our auditors have a duty to review our records in a fair and accurate manner. You are expected to cooperate with independent and internal auditors in good faith and in accordance with law. In addition, you must not fraudulently induce or influence, coerce, manipulate or mislead our independent or internal auditors regarding financial records, processes, controls or procedures or other matters relevant to their engagement.

Obligation to Investigate and Report Potential Violations

You should make appropriate inquiries in the event you may see, for example:

- financial results that seem inconsistent with underlying business performance;

- inaccurate financial records, including travel and expense reports, time sheets or invoices;

- the circumventing of mandated review and approval procedures;

- transactions that appear inconsistent with good business economics;

- the absence or weakness of processes or controls; or

• persons within the company or any affiliate seeking to improperly influence the work of our financial or accounting personnel, or our external or internal auditors.

Dishonest or inaccurate reporting can lead to civil or even criminal liability and fines and/or imprisonment for you and the company or its affiliates and can lead to a loss of public faith in the company or its affiliates. You are required to promptly report any case of suspected financial or operational misrepresentation or impropriety. If you believe that questionable accounting or auditing conduct or practices have occurred or are occurring, you should notify the company. Examples of questionable accounting or auditing conduct or practices may include, without limitation:

• significant deficiencies in the design or operation of internal controls or procedures that could adversely affect the company's or its affiliates' ability to record, process, summarize or report financial data;

• any evidence of fraud that involves an employee who has a significant role in the company's or its affiliate's financial reporting, disclosures or internal controls or procedures; or

• any evidence of a material violation of the policies in this Code regarding financial reporting.

SAFEGUARDING ASSETS

Overview

All employees, agents, consultants and contractors are responsible for the proper use of assets of the company and its affiliates. This responsibility applies to all assets, including your time, work and work product; cash and accounts; physical assets such as inventory, equipment, vehicles, computers, systems, facilities and supplies; intellectual property, such as patents, copyrights, trademarks and trade secrets; and other proprietary or nonpublic information.

- You should use all reasonable efforts to safeguard assets against loss, damage, misuse or theft.

- You should be alert to situations that could lead to loss, damage, misuse or theft of company assets, and should report any loss, damage, misuse or theft as soon as it comes to your attention.

- You should not use, transfer, misappropriate, loan, sell or donate assets without appropriate authorization.

- You must take reasonable steps to ensure that the company or its affiliate(s) receives good value for funds of the company or affiliate(s) spent.

- You may not use assets of the company or any affiliate in a manner that would result in or facilitate the violation of law.

- You should use and safeguard assets entrusted to the custody of the company or any affiliate by customers, suppliers and others in the same manner as assets of the company or any affiliate.

Protecting Information

In the course of your involvement with the company or any affiliate, you may come into possession of information that has not been disclosed or made available to the general public. This nonpublic information may include, among other things:

- financial data and projections;

- proprietary and technical information, such as trade secrets, patents, inventions, product plans and customer lists;

- information regarding corporate developments, such as business strategies, plans for acquisitions or other business combinations, divestitures, major contracts, expansion plans, financing transactions and management changes;

- personal information about employees; and
- nonpublic information of customers, company consortium members, vendors and others.

If you have any questions as to what constitutes nonpublic information, please consult the Compliance Manager in the Department of Global Operations of Airports Worldwide, Inc.

All nonpublic information must only be used for the business purposes of the company and its affiliates. You have an obligation to use all reasonable efforts to safeguard such nonpublic information. You may not disclose nonpublic information to anyone outside of the company or its affiliates, except when disclosure is required by law or when disclosure is required for business purposes and appropriate steps have been taken to prevent misuse of that information. This responsibility includes not disclosing nonpublic information in Internet discussion groups, chat rooms, bulletin boards or other electronic media. The misuse of nonpublic information is contrary to company policy and may also be a violation of law.

Employees, agents, consultants, and contractors are required to comply with the provisions above regarding the use of information belonging to the company and its affiliates. In addition to these provisions, you may have signed a confidentiality or nondisclosure agreement with the company or its affiliates. You are required to comply with the terms of any such confidentiality or nondisclosure agreement in addition to the provisions set forth in this Code. To the extent the provisions in this Code conflict or overlap with your confidentiality or nondisclosure agreements, the agreements govern.

Prohibition on Insider Trading

Although neither company nor any of its affiliates are currently a public company, at any time the company or an affiliate may elect to become publicly traded by filing a public registration statement. In such event, additional civil and criminal restrictions on insider trading will apply. For example, you may not directly or indirectly buy or sell stocks or other securities of a public reporting company based on nonpublic information obtained from your work at the company. Insider trading rules are strictly enforced, even in instances when the financial transactions seem small. If you have any questions at all regarding trading in securities of the company or any affiliate, contact the Compliance Manager of Airports Worldwide, Inc.

Maintaining and Managing Records

The company and its affiliates are required by local, state, U.S. federal, foreign and other applicable laws, rules and regulations to retain certain records and to follow specific guidelines in managing its records. Records include paper documents, email, compact discs, computer hard drives, floppy disks, microfiche, microfilm and all other recorded information, regardless of medium or characteristics. Civil and criminal penalties for failure to comply with such guidelines can be severe for employees, agents, consultants, contractors and the company and its affiliates. You will be notified if a legal hold is placed on records for which you are responsible. A legal hold suspends all document destruction procedures in order to preserve appropriate records under special circumstances, such as litigation or government investigations. If a legal hold is placed on records for which you are responsible, you must preserve and protect the necessary records. Records or supporting documents that are subject to a legal hold must not be destroyed, altered or modified under any circumstance. A legal hold remains effective until it is officially released in writing.

WORKING WITH OTHERS

Overview

You should respect the rights of, and deal fairly with, the customers, vendors, business associates and competitors of the company and its affiliates in compliance with law. You should not take unfair advantage of anyone through deception, misrepresentation, manipulation, coercion, abuse of privileged information or any intentional unfair business practice.

Foreign Corrupt Practices Act Compliance

The company and its affiliates will conduct every business transaction (including without limitation, operations, negotiations, and marketing) with integrity and will comply with: (a) the laws and regulations of the United States, particularly the provisions of the Foreign Corrupt Practices Act ("FCPA"); (b) the laws and regulations of each foreign country in which the Company operates or is looking to operate, including the provisions of the UK Bribery Act; (c) all international anti-bribery and corruption conventions; and (d) this Code.

The provisions of this section of the Code will apply to all employees of the company and its affiliates worldwide. In addition, the company requires independent third parties who represent the company or its affiliates (such as agents, consultants, contractors, and members of a company consortium) to conduct themselves in a manner consistent with this section of the Code.

Failure to comply with this section may result in significant civil and criminal penalties for the company, its affiliates and the individuals involved and is cause for disciplinary action against such individuals, up to and including termination.

Summary of Key FCPA Provisions

The Foreign Corrupt Practices Act is a federal law: (i) prohibiting payment of bribes (broadly defined) to foreign officials, and (ii) requiring companies to keep accurate books and records.

All employees and third parties should remain vigilant in watching for, avoiding and reporting to the Compliance Manager of Airports Worldwide, Inc. any questionable transactions.

1. Anti-Corruption/Bribery

A. In General - Under the FCPA's anti-bribery provisions, the company, its affiliates and their respective officers, employees and agents are prohibited from giving, offering, or promising anything of value to any foreign (non-U.S.) official, with the intent to obtain or retain business or any other advantage. This prohibition should be interpreted broadly.

The following concepts are essential to understanding the scope of the prohibition:

• Companies and individuals may be held liable for violating the anti-bribery provisions of the FCPA whether or not they took any action in the U.S. Therefore, a U.S. company, and individuals, employees, or officers, can be liable for the conduct of its overseas employees or agents, even if no money was transferred from the U.S. and no U.S. person participated in any way in the foreign bribery.

• A "foreign official" means any officer or employee of a foreign government, regardless of rank, employees of government-owned or government-controlled businesses, foreign political parties, party officials, candidates for political office, and employees of public international organizations. For the purposes of the FCPA, government-owned or government-controlled businesses include businesses where a foreign government is a shareholder, even if the foreign government is a minority shareholder. Public international organizations are designated by Executive Order of the President of the United States from time to time, and include organizations such as the United Nations, the World Bank, and the International Red Cross. The term “foreign official” can also include operator employees where the operator is a national company in the country of operations.

• "Giving, offering or promising" includes direct and indirect payments, gifts, offers, or promises. Even if the improper payment is not consummated, just offering it violates the FCPA. Likewise, instructing, authorizing, or allowing a third party to make a prohibited payment on the company’s or an affiliate's behalf, ratifying a payment after the fact, or making a payment to a third party knowing or having reason to know that it will likely be given to a government official constitute FCPA violations. The fact that a foreign official initially suggests or demands the payment is not considered a defense.

• "Anything of value" includes not only cash and cash equivalents, but also gifts, entertainment, travel expenses, accommodations, reimbursements for expenses, stock options, positions in joint ventures, subcontracts, and anything else of tangible or intangible value. See below for Hospitality Guidelines on when gifts and entertainment are permitted.

• "To obtain business or any advantage" includes for example an award of contract or preventing contract termination, a reduction in taxes or penalties, a favorable change in regulations, tolerance of non-compliance with local rules, or other favors or preferential treatment. The business to be obtained or retained does not need to be with a foreign government or foreign government instrumentality.

2. Record Keeping and Account Provisions – Under the FCPA, companies are required to: "Make and keep books, records, and accounts which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of assets" of the company. "Records" includes virtually all forms of business documentation, including accounts, correspondence, memorandums, tapes, discs, papers, books, and other documents or transcribed information of any type. This applies to all payments, not just sums that would be "material" in the traditional financial sense.

3. Penalties & Fines – The FCPA is aggressively enforced by the Department of Justice and the Securities and Exchange Commission, and criminal and civil penalties may be assessed against both individuals (including jail time) and companies that violate FCPA. Individual employees of a company may be prosecuted even if the company for which they work is not. The following set forth some of the criminal and civil penalties that can result from violating the FCPA:

- Violations of the anti-bribery provisions can result in individual criminal penalties of up to $100,000.00 USD per violation and/or imprisonment for up to five (5) years per violation. Individual civil penalties can include fines of up to $16,000.00 USD per violation.

- Violations of the anti-bribery provisions can also result in criminal fines of up to $2 million USD per violation for the company, and civil fines of up to $16,000.00 USD per violation.

- Violations of the record keeping and accounting provisions can result in individual criminal penalties of up to $5 million USD per violation and/or imprisonment for up to twenty (20) years per violation. Individual civil penalties range from $7,500.00 USD to $150,000.00 USD per violation.

- Violations of the record keeping and accounting provisions can also result in criminal fines of up to $25 million USD per violation for the company, and civil penalties can range from $75,000.00 USD to $750,000.00 USD per violation.

4. It is important to remember that the FCPA does permit doing business with foreign (non-U.S.) governments, departments, agencies, and government-owned or controlled companies so long as the business is conducted at arms-length, is transparent, is based upon fair market value, and is in compliance with the FCPA. However, given the risks inherently present when conducting business with foreign governments, great care must be exercised to ensure compliance with the FCPA. **Any and all questions regarding compliance with the FCPA and any other anti-bribery laws, regulations, and conventions should be directed to the Compliance Manager.**

Summary of Key UK Bribery Act Provisions

The UK Bribery Act is a British law that prohibits the payment of bribes. It applies not only to citizens of the United Kingdom ("UK"), residents and companies, but also to non-UK companies who conduct business in the UK. A company can be liable for violations committed for its benefit by its employees, affiliates, and independent third parties who represent the company. A company can be prosecuted even if it has no knowledge of the relevant actions. Similar to the FCPA, both individuals and companies can be prosecuted for violating the UK Bribery Act even if the violation occurred outside the UK.

Like the FCPA, the UK Bribery Act prohibits improper payments to foreign officials. However, the UK Bribery Act is broader than the FCPA, as it also prohibits non-government individuals and entities from offering, paying or receiving payments intended to induce proper performance of a "relevant function or activity." "Relevant functions or activities" include bribes that are offered or paid in connection with purely commercial activities, such as securing supplies or new business contracts.

The UK Bribery Act's ban on all forms of bribery also extends to activities that are "connected with business, performed in the course of a person's employment or performed on behalf of the company" for which performance is expected by undertaken in good faith, impartially, or from a position of trust.

Like the FCPA, all employees and third parties should remain vigilant in watching for, avoiding and reporting to the Compliance Manager of Airports Worldwide, Inc. any questionable transactions.

Implementation Procedure – Operational Directives

1. Except as provided in this Code, no offer, payment, promise to pay or authorization to pay or provide any money, gifts or anything of value will be made by or on behalf of the company or any affiliate to:

- Any foreign official, regardless of rank (see definition in paragraph 1(A)(2) above); or

- Any person, while knowing or being aware of a high probability that all or a portion of any payment will be offered, given or promised, directly or indirectly, to a foreign official.

Further, except as provided in this Code, no employee shall, for the purpose of securing an improper advantage for the company and its affiliates, offer or promise, or make or facilitate a payment or gift of anything of value to or accept anything of value from any person.

2. The company requires independent third parties who represent the company or its affiliates to conduct themselves in a manner consistent with this section.

3. The company and its affiliates will exercise care and perform due diligence in selecting such third parties by employing only reputable entities and will pay only reasonable compensation for the services provided. Reasonable documentation must accompany all requests for payment to third parties, and the company, its affiliates, and its employees will not make payments to any third party where there is a suspicion that that third party could make illicit or questionable payments or gifts.

4. The company and its affiliates shall not make contributions to political parties or committees or to individual politicians without the prior written consent of the Chief Executive Officer of the company. Approved contributions may only be made in accordance with the applicable law, and all requirements must be fully complied with for public disclosure of such contributions.

5. The making of improper charitable contributions on behalf of foreign officials may have severe consequences under the FCPA and the UK Bribery Act for the company, its affiliates and involved employees. In no instance may an employee or a business segment make a donation payment at the behest of a foreign official or to an organization affiliated with a foreign official or his close relatives without first obtaining approval from the Chief Executive Officer. If a donation is made, it must be accurately described in the books and records of the company.

6. No one acting for or on behalf of the company or any affiliate shall enter into any business arrangement with an independent third party, unless the third party warrants compliance with this Code and all applicable anti-corruption, including commercial bribery, laws and regulations.

Implementation Procedure – Financial and Accounting Directives

The Chief Financial Officer of Airports Worldwide, Inc. ensures that the accounting and recordkeeping activities of the company comply with applicable law and conform to this section of the Code. However, each officer and employee involved with financial and accounting functions must be alert to possible violations of the following Financial and Accounting Directives and will report suspected violations to the Compliance Manager.

1. All cash, bank accounts, investments and other assets of the company and any affiliates must always be recorded accurately on the official books of the company and its affiliates. In accordance with this section of the Code and the company's internal control structure, the Board of Directors will periodically review such books, records, and controls to ensure their compliance with the requirements of the FCPA. No employee shall falsify any accounting or other business record, and all employees shall respond truthfully and fully to any questions from the internal or independent auditors of the company or any affiliate.

2. Bank accounts should be opened or closed only upon the prior written approval of the Chief Financial Officer of Airports Worldwide, Inc. Anonymous ("numbered") accounts will not be maintained.

3. Payments will not be made into anonymous bank accounts or other accounts not in the name of the payee or of any entity known to be controlled by the payee.

4. Except for regular, approved payroll payments or normal disbursements from petty cash supported by signed receipts or other appropriate documentation, payments will not be made in cash. Checks will not be drawn to the order of "cash," "bearer" or similar designations.

5. Fictitious invoices, over-invoices or other misleading documentation will not be used.

6. Fictitious entities, sales, purchases, services, loans or financial arrangements will not be used.

7. Check requests will be in writing and contain a complete explanation of the purpose and authority for the payment. The explanation will accompany all documents submitted in the course of the issuing process and will be kept on file.

8. No expenses relating to foreign business will be reimbursed to persons or companies assisting the company or affiliates in obtaining or retaining such business unless such expenses are supported by reasonable written documentation.

9. No payment to any consultant will be made outside of either a) the US, or b) the country where a substantial portion of the related services are performed, or c) the country from which the person performing such services normally conducts business.

10. Payments for any services rendered to the company or an affiliate by a foreign official (including an officer of a foreign government-owned or controlled commercial enterprise), including honorarium payments and reimbursement of expenses, will be made solely to the foreign government agency or instrumentality employing the individual. Such payments will be made by check directly to the foreign government agency or instrumentality, or by wire to its named bank account within the foreign government agency’s or instrumentality’s country, or by wire through its duly authorized correspondent bank within the U.S. No such payment shall be made without the prior written approval of the Chief Executive Officer.

11. Receipts, whether in cash or checks, will be deposited promptly in a bank account of the Company. Any employee who suspects the possibility that a bribe, kickback or over-invoice is associated with a particular receipt or that an understanding exists that all or a portion of a receipt will be rebated, refunded or otherwise paid in contravention of the laws of any jurisdiction, will immediately report that suspicion to the Compliance Manager.

Implementation Procedure – Hospitality Guidelines

These guidelines are to be followed for activities involving foreign government officials or employees in all countries.

1. All hospitality in the form of entertainment and gifts offered on behalf of the company or any affiliate must be directly related to business of the company and its affiliates. Hospitality in all cases must be reasonable in amount, must be offered in good faith only in connection with the promotion, demonstration or explanation of company products or services or the execution or performance of a contract with a foreign government or agency thereof, and must be lawful under applicable local law. All hospitality must receive the prior approval of the Chief Executive Officer. **In no event may any hospitality be offered or provided in return for any favor or benefit to the company or its affiliates or to influence improperly any official decision.**

2. Subject always to the approval of the Chief Executive Officer of the company in writing, expenses for hospitality meals may not exceed the following U.S. dollar amount per person:

Breakfast: $30.00
Lunch: $50.00
Dinner: $100.00

Refreshments unaccompanied by a meal should not exceed $50.00 per person.

3. Frequency of hospitality must be carefully monitored, as the cumulative effect of frequent hospitality may give rise to the appearance of impropriety. Hospitality for an individual should be "infrequent" and not exceed twelve events in any calendar year.

4. Cash gifts to foreign officials are not permitted under any circumstances and any gift or entertainment which under the circumstances would constitute "Prohibited Payments" or "Commercial Bribery" (as such terms are defined under the FCPA) are forbidden regardless of amount or frequency. Per diem payments to foreign officials are similarly prohibited.

5. Promotional items of nominal value such as coffee mugs, calendars, or similar items, or items displaying the company logo that are distributed for advertising or commemorative purposes, or gifts of nominal value on customary holidays are permitted. "Nominal value" is $100.00 or less.

6. In the event the company or its affiliate is responsible for the airfare or lodging expenses of a foreign official, itineraries and any other supporting documentation shall be maintained. In no case will payment or reimbursement be made directly to the individual official incurring the expense; such payment or reimbursement shall only be made directly to the service provider (i.e. the airline) or the foreign government or agency involved. Expenses beyond what is reasonably necessary for the business purpose, including lavish accommodations or expenses for spouses and children, will not be approved. **The Chief Executive Officer of the company or his designee must approve all travel and lodging for foreign officials in advance of the trip.**

7. In all cases that entertainment, gifts, or travel expenses are approved, the expenses must be supported by receipts and accurately recorded in the books and records of the company and its affiliates, as applicable.

Implementation Procedure – Due Diligence Process for International Consultants & Agents

1. No employee of the company or any affiliate may retain an international intermediary until sufficient due diligence has been performed to enable the company to conclude with reasonable assurance that the consultant, agent, or intermediary understands and will fully abide by the FCPA, the UK Bribery Act, and this Code. An "intermediary" for these purposes is any agent, consultant, vendor, government service provider (companies that provide local customs clearance, visa, legal or other regulatory services), joint venture partner, or any other person or entity who will interact with a foreign official on behalf of the company or any affiliate.

2. If you are considering retaining an intermediary, please contact the Compliance Manager of Airports Worldwide, Inc. who will promptly begin the due diligence process.

Red Flag Awareness

You must not deliberately ignore circumstances that should reasonably alert you to possible violations of the FCPA or the UK Bribery Act.

Willful ignorance of facts which indicate possible violation of the Code will equate to "Knowing" the facts under the FCPA. "Knowing" means having actual knowledge or reasonable grounds to believe that facts or circumstances exist. For example, if there are reasonable grounds to believe that some or all of a payment to a third party will be used to make a Prohibited Payment to a Government Official, the person making the payment to the third party will be deemed to have made the payment to the third party with knowledge of the third party's intention.

Knowledge can be inferred from "willful blindness" to, or "conscious disregard" of, facts and circumstances. This means that a person will be considered to have knowledge and to have acted knowingly if there is evidence of a conscious purpose to avoid learning the truth.

In evaluating potential intermediaries and during any relationship with them, employees of the company or its affiliates must be conscious of any "red flags" that may be present or arise. A "red flag" is a fact or circumstance that serves as a warning signal that an intermediary may act corruptly. It is the responsibility of the employee that observes a red flag to refer the matter to the Compliance Manager of Airports Worldwide, Inc. A non-exclusive list of examples of red flags is below:

- rumors regarding unethical or suspicious conduct by an employee, marketing representative, consultant, agent, or other business partner, or by a government official;

• unnecessary third parties or multiple intermediaries;

• requests for payments to a third party rather than the consultant or agent;

• requests for payments in a third country;

• business in a country with bribery problems (Examples of countries with a history of bribery problems include, but are not limited to Nigeria, Kazakhstan, Haiti, Myammar, Iraq, Guinea, Sudan, Congo, Chad, Bangladesh, Uzbekistan, Equatorial Guinea, Cote d'Ivoire, Cambodia, Venezuela, Argentina, Sierra Leone, Pakistan, Egypt, Ecuador, Bolivia & Kenya);

• requests for payments in cash;

• requests for unusually large commissions or other payments, or payments that appear excessive for the service rendered

• political contributions;

• requests for reimbursement of expenses that are poorly documented;

• relation to or a close association with a foreign official;

• incomplete or inaccurate information in required disclosures; or

• refusal to certify compliance.

Once a potential third party has been retained, the company, its affiliates, and its employees will monitor the third party's expenses and activities to ensure compliance with this Code. Failure to monitor a third party for continued compliance with the FCPA can result in FCPA liability. It is the responsibility of any employee that observes a retained third party's non-compliance with this Code, the FCPA, and all other applicable anti-bribery laws, regulations, and conventions to immediately refer the matter to the Compliance Manager of Airports Worldwide, Inc.

Selecting Vendors

The company's policy is to select vendors based on the merits of their products, services and business practices and to purchase supplies based on need, quality, service, price and other terms and conditions of sale. You may not establish a business relationship with any vendor if you know that its business practices violate applicable laws.

Handling the Nonpublic Information of Others

You must handle the nonpublic information of others responsibly and in accordance with our agreements with them. Nonpublic information of others includes notes, reports, conclusions and other materials prepared by a company employee based on the nonpublic information of others.

Even after a nondisclosure agreement is in place, you should accept only the information that is necessary or appropriate to accomplish the purpose of receiving it, such as a decision on whether to proceed to negotiate a deal. If more detailed or extensive information is offered and it is not necessary or appropriate for your immediate purposes, it should be refused. If any such information is inadvertently received, it should be transferred to the Compliance Manager for appropriate disposition.

Once the company or any affiliate has received nonpublic information, you should use all reasonable efforts to:

- abide by the terms of the relevant nondisclosure agreement, including any obligations with respect to the return or destruction of the nonpublic information;

- limit the use of the nonpublic information to the purpose for which it was disclosed; and

- disseminate the nonpublic information only to those other employees, agents or contractors of the company or its affiliates with a need to know the information to perform their jobs for the company or any of its affiliates.

Improperly Obtaining or Using Assets or Information

You may not unlawfully obtain or use the materials, products, intellectual property, proprietary or nonpublic information or other assets of anyone, including suppliers, customers, business partners and competitors. You may not coerce or improperly induce past or present employees of other companies to disclose proprietary or nonpublic information of their former or other employers.

Free and Fair Competition

It is our policy to lawfully compete in the marketplace. Our commitment to fairness includes respecting the rights of our competitors to compete lawfully in the marketplace and abiding by all applicable laws in the course of competing.

Most countries have well-developed bodies of law designed to encourage and protect free and fair competition. These laws are broad and far-reaching and regulate the relationships of the company and its affiliates with its vendors, resellers and customers. Competition laws generally address the following areas: pricing practices (including predatory pricing, price fixing and price discrimination), discounting, terms of sale, credit terms, promotional allowances, secret rebates,

exclusive dealerships or distributorships, product bundling, restrictions on carrying competing products, termination and many other practices.

Competition laws also govern, usually quite strictly, relationships between the company, its affiliates and their competitors. Collusion among competitors is illegal, and the consequences of a violation are severe. You must not enter into an agreement or understanding, written or oral, express or implied, with any competitor concerning prices, discounts or other terms or conditions of sale; profits or profit margins; costs; allocation of product, customers, markets or territories; limitations on production or supply; boycotts of customers or suppliers; or bids or the intent to bid, or even discuss or exchange information on these subjects.

The company and its affiliates are committed to obeying both the letter and spirit of these laws, which are often referred to as antitrust, consumer protection, competition or unfair competition laws. Although the spirit of these laws is straightforward, their application to particular situations can be quite complex. To ensure that the company and its affiliates comply fully with these laws, you should have a basic knowledge of them and should promptly involve our Chief Executive Officer of the Company and Compliance Manager when questionable situations arise.

Anti-Terrorism

A number of countries, including the United States, have enacted strict anti-money laundering and anti-terrorism laws and regulations. Many of these laws and regulations require reporting of suspicious transactions and activities. All persons and entities acting for or on behalf of the company or any of its affiliates must comply with all applicable anti-money laundering and anti-terrorism requirements and must report suspected violations and other questionable conduct to the Compliance Manager of Airports Worldwide, Inc.

All persons acting for or on behalf of the company shall not knowingly:

a. Engage in any financial transaction involving property, funds or monetary instruments which, directly or indirectly, promotes or results from criminal activity punishable under the laws of any country;

b. Receive, transfer, transport, retain, use, structure, divert, or hide the proceeds of any criminal activity, or aid or abet another in any such action;

c. Engage or become involved in, finance or support financially, or otherwise sponsor, facilitate, or assist any terrorist person, activity, or organization; and

d. Aid, abet or otherwise become involved in any arrangement that would result in a violation of this Code by any person.

Any questions of concern with respect to compliance with the requirements of these laws and regulations must be addressed to the Compliance Manager of Airports Worldwide, Inc.

Economic Sanctions Law

The governments of many of the countries in which the company or any of its affiliates conducts business, and many organizations formed by states, governments or other international organizations formed by states, governments or other international organizations such as regional economic integration organizations like the European Union, the OECD, the World Bank, or the United Nations, have imposed economic and trade sanctions against selected countries to further foreign policy, national security and other objectives. Some of these sanctions have been unilateral, while others have been imposed multi-nationally.

The sanctions programs vary in scope. Some are selective, prohibiting a specific class of economic transactions, such as transactions with the sanctioned government only. Others are comprehensive, prohibiting all transactions involving the sanctioned country, its nationals, wherever they are located in the world, or anyone physically located within a sanctioned country regardless of nationality. Laws implementing these sanctions impose obligations on companies by ordering the freezing of assets of, and by prohibiting the company's dealings with, embargoed parties.

U.S. sanctions generally apply to all operations of U.S. companies, including overseas branches, affiliates and subsidiaries of such companies, and to all U.S. nationals wherever they may be located. Other countries joining an economic embargo will often impose sanctions that are somewhat different in scope from those imposed by the United States. In such situations, an overseas company office may be subject to both the U.S. sanctions and any sanctions established by the country in which it is located. However, some foreign countries, not subscribing to economic sanctions or embargo, actually prohibit branches, affiliates and subsidiaries of U.S. firms located in such countries from complying with U.S. sanctions. These situations involve complex legal questions and, accordingly, must be carefully examined by the Compliance Department of Airports Worldwide, Inc.

Any questions of concern with respect to compliance with the requirements of these laws and regulations must be addressed to the Compliance Manager of Airports Worldwide, Inc.

International Trade Compliance

It is the company's policy to comply strictly with all applicable international trade control laws and regulations of the United States and all jurisdictions in which the company conducts business (to the extent that compliance with local laws does not conflict with U.S. legal requirements).

The United States imposes rigorous international trade control standards to which the company, including its non-U.S. operations, must adhere. These laws and regulations cover the export and re-export of products, services, software, technology, and technical data, sanctions, and anti-boycott requirements.

The United States also maintains several lists of persons and entities with whom U.S. companies cannot do business, and personnel should routinely check vendors, project partners, subcontractors and other parties against those lists when engaging in international transactions. Additionally, most other countries in the world impose similar controls on the export of goods from within their jurisdictions.

Failure to observe export control laws, sanctions and anti-boycott requirements can severely damage the company's reputation and may subject the company and its affiliates to criminal and civil fines and loss of export privileges, and individuals to fines and imprisonment. Non-compliance with the applicable rules by company employees could result in corporate discipline, including dismissal. Employees whose work involves the sale, shipment, electronic transfer or disclosure of technical information, software, goods or services across national borders are required to keep up to date with applicable rules and regulations. Employees must seek guidance from the Compliance Manager of Airports Worldwide, Inc. whenever the legality or propriety of any prospective transaction or course of conduct is subject to question or doubt. Additionally, in the event that any employee receives any proposed agreements from potential customers or vendors that contain any boycott language this must be immediately disclosed to the Compliance Manager of Airports Worldwide, Inc.

To ensure proper compliance with all export regulations, company employees must educate themselves about export compliance issues, which includes, at a minimum, taking the following steps:

- Know your customer – who they are, what they do, where they are based, and how they will use your goods, technology or software;
- Attend export compliance training sessions when offered by the company to keep up to date with changes in the rules;
- Be aware of which countries have been sanctioned by the United States government (currently Burma, Cuba, Iran, North Korea, Sudan and Syria – this list is subject to frequent change);
- Seek advice from the Compliance Manager if you have any doubts;
- Remember that an export can be made electronically, through discussions and by visual inspection, as well as by traditional shipping methods; and
- Think carefully about the potential impact of export control laws and sanctions before transferring goods, technology or software across national borders.

Examples of export-controlled items that may be subject to export controls include:

- Advanced airplane fire suppression equipment
- Advanced airport security screening equipment
- Laptop computers procured in the United States
- Personal protective equipment such as helmets and vests used to protect personnel in areas with security risks
- Transfer of technical data relating to export controlled equipment or transfer of software outside the United States or to foreign nationals within the United States

The above list is intended to be illustrative and contains just some of the many different goods, products, and data that could be subject to export regulation.

Each employee is required to understand and comply with the international trade control laws and regulations as they apply to his or her job activities. The company's Compliance Manager is available to provide guidance, and employees should contact this office if they have any questions or concerns about compliance with international trade control laws and regulations. The Compliance Manager will take appropriate action as outlined in the memorandum and recommendation from Hughes Hubbard & Reed, LLC dated July 20, 2010 (Exhibit A) which may include additional compliance guidance from outside legal counsel.

The company shall establish and maintain a continuing program to keep its employees advised of the applicable provisions of the international trade control laws, regulations and requirements. Any employee with a question concerning international trade control laws and regulations shall refer the question to the company's Compliance Manager.

WORKING WITH GOVERNMENTS

Overview

Employees, agents, consultants and contractors of the company and its affiliates should use all reasonable efforts to comply with all applicable laws and regulations governing contact and dealings with governments, government employees and public officials. If you deal with governments, government employees or public officials, you should undertake to understand the special rules that apply. If you have any questions concerning government relations, you should contact the Compliance Manager.

Government Contracts

You should use all reasonable efforts to comply with all relevant laws and regulations that apply to government contracting. You should refer all contracts with any governmental entity to the Compliance Manager for review and approval.

Requests by Regulatory Authorities

You must cooperate with appropriate government inquiries and investigations in accordance with law. It is important, however, to protect the legal rights of the company and its affiliates with respect to its nonpublic information. All government requests for company information, documents or investigative interviews should be referred to the Compliance Manager. You should work with the Compliance Manager in responding to requests by regulatory authorities to ensure adequate and complete responses and to avoid improper disclosure of attorney-client privileged materials, trade secret information or other nonpublic information. This policy should not be construed to prevent an employee from disclosing information to a government or law enforcement agency, where the employee has reasonable cause to believe that the information discloses a violation of, or noncompliance with, a state or federal statute or regulation.

Political/Charitable Contributions

It is the company's policy that contributions to political parties, candidates and campaigns for public office, or charities made on behalf of the Company must be authorized in writing, in advance, by the Chief Executive Officer or his designated represented for such purposes.

Employees of the company or any affiliate, acting solely for themselves, are neither encouraged nor discouraged from making contributions to political parties, candidates or campaigns for public office or charities.

All political and charitable contributions must comply with applicable laws and regulations.

Contributions to political parties, candidates or charities by employees of the company or its affiliates, acting solely for themselves, may not involve the use of funds, time, equipment, supplies or facilities of the company or its affiliates.

In the event that employees of the company or any affiliate address political issues in their individual capacities, they must state explicitly that they are not speaking or acting on behalf of the company or the affiliate, as applicable.

A contribution to a political party, a candidate or campaign for public office, or a charitable contribution that could be construed as being a Prohibited Payment is prohibited regardless of the intent of the donor.

PROCEDURAL MATTERS

Distribution

All employees will receive a copy of this Code at the time they join the company or an affiliate of the Company and will receive periodic updates. Agents, consultants, contractors and members of company consortium shall also be provided with a copy of the Code.

Acknowledgment

All new employees must sign an acknowledgment form confirming that they have read the Code and that they understand and agree to comply with its provisions. A copy of the signed acknowledgment form will be kept in your personnel file. Failure to read the Code or to sign an acknowledgement form does not excuse any person from the terms of the Code.

Reporting Violations

You should promptly report violations or suspected violations of this Code to the Compliance Manager by calling +1 (832) 626-4716 (from inside the United States) or +011 (832) 626-4716 (from outside the United States) or online at www.adchas.ethicspoint.com or through the hotline +1-855-761-0365. If your situation requires that your identity be kept secret, your anonymity will be preserved to the greatest extent reasonably possible. If you wish to remain anonymous, send a letter addressed to the company, attention: the Compliance Manager, Airports Worldwide, Inc., at 15600 JFK Blvd., Suite 110, Houston, Texas USA 77032 or utilize the website and/or hotline. If you make an anonymous report, please provide as much detail as possible, including copies of any documents that you believe may be relevant to the issue.

If your concerns relate to accounting, internal controls or auditing matters, , you may also contact the Chief Financial Officer of the company at 15600 JFK Blvd., Suite 110, Houston, Texas USA 77032. If the Compliance Manager is implicated in any violation or suspected violation, you may contact the Chief Financial Officer at 15600 JFK Blvd., Suite 110, Houston, Texas USA 77032. Reprisals, threats, retribution or retaliation against any person who has in good faith reported a violation or a suspected violation of law, this Code or other company policies, or against any person who is assisting in any investigation or process with respect to such a violation, is prohibited.

Investigations

The Board of Directors of the company or its designated committee will be responsible for investigating violations and determining appropriate disciplinary action for matters involving members of the Board of Directors or executive officers. The Board of Directors or its designated committee may designate others to conduct or manage investigations on its behalf and recommend disciplinary action.

Subject to the general authority of the Board of Directors to administer this Code, the Chief Executive Officer of the company will be responsible for investigating violations and determining appropriate disciplinary action for other employees, agents, consultants, contractors and members of company consortium. The Chief Executive Officer of the company may designate others to conduct or manage investigations on their behalf and recommend disciplinary action. The Chief Executive Officer will periodically report Code violations and the corrective actions taken to the Board of Directors or its designated committee. The Board of Directors reserves the right to investigate violations and determine appropriate disciplinary action on its own or to designate others to do so in place of, or in addition to, the Chief Executive Officer.

The company and its affiliates will promptly investigate any suspected violations. If it is determined that evidence of a violation exists, the individual subject to investigation will be notified. The subject of an investigation will have an opportunity to respond to any allegations made against that person. A person suspected of violating the Code may be suspended with or without pay while an investigation is conducted. The company and its affiliates will follow local grievance procedures in jurisdictions where such procedures apply.

Disciplinary Action

The company and its affiliates will take appropriate action against any employee, agent, consultant, contractor or member of a company consortium whose actions are found to violate the Code. Disciplinary action may also result from:

a. Condoning or failing to report a known or suspected violation of the Code, or other illegal, improper or unethical conduct; or

b. Failing to execute, or falsifying, any required certification; or

c. Failing to cooperate fully, truthfully, and candidly with a compliance review or an investigation of reported suspected violation of the Code; or

d. Failing to perform adequate due diligence with respect to the engagement of any agent, representative, vendor, and government services provider.

Disciplinary actions may include oral or written reprimand, suspension or immediate termination of employment or business relationship, or any other disciplinary action or combination of disciplinary actions as deemed appropriate to the circumstances. A record of the disciplinary action will be retained in the employee's personnel file.

In determining what disciplinary action is appropriate in a particular case, the company and its affiliates will take into account all relevant information, including the nature and severity of the violation, any history of warnings and violations, whether the violation appears to have been intentional or inadvertent and whether the violator reported his or her own misconduct. The company and its affiliates will strive to enforce the Code in a consistent manner while accounting for all relevant information. An alleged violator may make a written request for reconsideration within 14 days of notification of the final disciplinary decision.

Where the company or any affiliate has suffered a loss, it may pursue its remedies against the individuals or entities responsible. Certain violations of this Code may also be subject to civil or criminal prosecution by governmental authorities and others and may result in imprisonment. Where laws have been violated, the company will report violators to the appropriate authorities.

ADDITIONAL INFORMATION

Nothing in this Code creates or implies an employment contract or term of employment. Employment at the company is employment at-will. Employment at-will may be terminated with or without cause and with or without notice at any time by the employee or the company. Nothing in this Code shall limit the right to terminate employment at-will. No employee of the company has any authority to enter into any agreement for employment for a specified period of time or to make any agreement or representation contrary to the company's policy of employment at-will.

The policies in this Code do not constitute a complete list of company policies or a complete list of the types of conduct that can result in discipline, up to and including discharge.

From time to time, directives pursuant to this Code may be issued. These directives may include requirements not imposed by this Code or may include waivers of compliance with certain requirements of this Code. It is your responsibility to ensure you are aware of, and comply with, all such contract-specific directives which are relevant to your job duties/location.

Hughes Hubbard & Reed LLP
1775 I Street, N.W.
Washington, D.C. 20006-2401
Telephone: 202-721-4600
Fax: 202-721-4646
hugheshubbard.com

Privileged and Confidential Attorney Work Product

EXHIBIT A: EXPORT COMPLIANCE MEMORANDUM

To: Wogbe Ofori
Senior Vice President, Global Operations
ADC & HAS Management Services, Inc.

July 20, 2010

From: Melissa L. Duffy
(Hughes Hubbard & Reed LLP)

cc: David Sheinbein
Ryan O. Cantrell
(Chamberlain, Hrdlicka, White, Williams & Martin)

Re: Potential U.S. Trade Compliance Issues for ADC & HAS Management Services, Inc.

I. Introduction

On June 24, 2010, Wogbe Ofori and Christine Leday of ADC & HAS Management Services, Inc. ("ADC & HAS") participated in a conference call with Ryan O. Cantrell of the law firm Chamberlain, Hrdlicka, White, Williams & Martin, and with Melissa L. Duffy of the law firm Hughes Hubbard & Reed LLP. The purpose of the call was to identify potential U.S. trade compliance issues involved in the regular business activities of ADC & HAS and to develop general recommendations in handling those issues.

Following the call, Mr. Ofori requested a written summary of the issues discussed, along with draft export compliance contractual language that could be used in purchase orders and subcontract agreements. This memorandum provides a discussion of potential U.S. trade compliance issues and recommendations, and it is intended for general issue-spotting purposes within ADC & HAS. The analysis of specific transactions with partners, customers, vendors or subcontractors would require a more detailed review of the information relevant to each situation. The draft contractual language is enclosed as an attachment to this memorandum.

II. Overview of ADC & HAS and Its Business Activities

Prior to and during the conference call, Mr. Ofori provided an overview of ADC & HAS and its business activities, which served as the basis for our discussion of potential U.S. trade compliance issues. Below is a summary of the information provided.

ADC & HAS provides airport operation and development services. ADC & HAS is based in Houston, Texas and is affiliated with the Houston Airport System ("HAS"). The principal

recipient of ADC & HAS' services is ADC & HAS Airports, Inc., a company which is organized in the British Virgin Islands and beneficially owned by HAS Development Corporation (the development affiliate of the Houston Airport System), Airport Development Corporation ("ADC") of Canada, and OMERS Strategic Investments. ADC & HAS specializes in airport privatization projects and provides development and operational expertise to such projects. The company offers management services, technical guidance, training, and software implementation services to its affiliates, which operate local privatized airports. At this time, 100% of its airport operations take place outside the United States.

The ADC & HAS core business includes the following activities:

A. Management Services

ADC & HAS advises its affiliates on the business management of their local airport operations. Specifically, ADC & HAS provides direction on accounting and finance, human resources, administration, marketing, government relations, security and law enforcement interface, and corporate operations. ADC & HAS generally provides its direction from Houston, with occasional site visits to the local facilities.

B. Technical Guidance, Support and Supervision

ADC & HAS provides technical guidance to affiliates in support of their local airport operations. ADC & HAS provides subject matter experts who consult with local personnel in areas relating to airport operations, facilities maintenance, environmental compliance, security, and social, health and safety requirements. In this case, "technical" refers to specialized business knowledge in airport operations and practices. ADC & HAS does not provide technical guidance in the areas of aircraft maintenance and operations, air traffic control, security equipment installation, maintenance or repair above a basic user level, or other areas involving specialized mechanical skill. Technical guidance, support and supervision are provided from Houston or at the local level.

C. Training

In addition to providing management direction and technical guidance to affiliates, ADC & HAS also trains local project personnel in the areas of airport operations, maintenance, safety and security. The training does not usually involve highly technical skills, such as aircraft maintenance or advanced security equipment repair; rather, the focus is on general airport operations. Project personnel generally come with some basic skills in the areas for which have been hired. Then, ADC & HAS teaches them how to perform their tasks according to the customized procedures of the company, at a company-wide standard of proficiency. This training takes place in Houston or at local projects.

D. Software Implementation

In general, ADC & HAS does not develop or export software. However, ADC & HAS' affiliate in Ecuador has developed a statistics software program, which the affiliate is considering

licensing to other ADC & HAS affiliates globally for internal company use. The purpose of this software is to track basic airport operations functions, such as the number of flights departing and arriving from the airport daily, and other business metrics on which airport performance is evaluated. As of this time, there has not been any U.S. collaboration or contribution to the software – its development has been entirely internal to the Ecuador affiliate. At a future time, there might be some U.S. input as the product is tested and improved for company-wide use, or if it is transferred to the United States for licensing. ADC & HAS does not intend to distribute or cause the distribution of the product outside its affiliated croup of companies.

E. Affiliate Activities

At the present time, due to the nature of the airport market, all of the airports managed by ADC & HAS are located in countries outside the United States, with a predominant emphasis on the Latin America region. The day-to-day operations of the airports are managed by local affiliates of ADC & HAS, which are indirect subsidiaries of ADC & HAS Airports, Inc. The subsidiaries maintain the physical buildings, roads, and other infrastructure, provide emergency response and firefighting services, interface with and assist government and contractor security forces, and manage the business aspects of operating the airports. The subsidiaries are also responsible for development, construction, and expansion of airport facilities. The subsidiaries are not involved in the operation or maintenance of aircraft or the administration of flight services. Similarly, the subsidiaries of ADC & HAS Airports, Inc. do not engage in air traffic control.

II. Potential Trade Compliance Issues

As noted above, the conference call on June 24, 2010 focused on identifying potential U.S. trade compliance issues that could be involved in the typical business activities of ADC & HAS. This section of the memorandum summarizes the issues that were discussed, along with the general recommendations that were presented for managing export compliance risk in those areas. The following discussion is intended to be used for general information-spotting purposes, with the understanding that specific situations will require a more detailed analysis based on a review of the relevant information.

A. Regulatory Background

1. U.S. Export Controls

Based on the information provided prior to and during the conference call, it appears that some of ADC & HAS' activities may be subject to the Export Administration Regulations ("EAR" – 15 C.F.R. Parts 730-774), which are administered by the U.S. Department of Commerce, Bureau of Industry and Security ("BIS"). The EAR regulate the export and re-export (*i.e.*, transfer from one non-U.S. country to another) of commercial and dual-use items. *See* 15 C.F.R. § 743.3. Other U.S. government agencies have jurisdiction over certain types of exports and re-exports, although ADC & HAS is less likely to encounter those export controls in its current daily business. For example, the export and re-export of munitions (*i.e.*, military) items is

governed by the International Traffic in Arms Regulations ("ITAR" – 22 C.F.R. Parts 120-130), which are administered by the U.S. Department of State.

Physical items, technology and software that are of U.S.-origin remain subject to export controls regardless of where in the world the items are located. Additionally, non-U.S. origin items located in the United States are subject to U.S. jurisdiction at the time they are directly exported from the United States. Under the EAR, a *de minimis* rule is used to determine whether items are U.S.-origin. *See* 15 C.F.R. § 734.4. Specifically, a foreign made item that incorporates at least 25% U.S.-origin content will itself be considered U.S.-origin for purposes of re-export controls. That threshold is lower – 10% U.S.-origin content – for items re-exported to anti-terrorism controlled countries (which currently include Cuba, Iran, North Korea, Sudan and Syria). Publicly available software and technical information, regardless of U.S.-origin content, are not controlled under the EAR. *See* 15 C.F.R. § 734.3(b)(3).

International companies can encounter export control issues when they engage in procurement activities involving U.S.-origin items, downloads of U.S.-origin software, and transfers of U.S.-origin technical information. U.S. export controls will apply, even if the procurement is taking place in a foreign country through local vendors, when the procured items are U.S.-origin (or if the items are foreign products that meet the *de minimis* U.S.-origin content threshold). Similarly, U.S. export controls will apply to in-country technology transfers to third country nationals or software downloads if the technology or software are U.S. origin, or if they meet the *de minimis* threshold.

The term "technology" has a very specific connotation within the EAR, which might be different from how that term is sometimes used in daily business. The EAR define "technology" as specific information necessary for the "development," "production," or "use" of a product, which takes the form of "technical data" or "technical assistance." 15 C.F.R. § 772 (definitions). ADC & HAS is a services provider and does not develop or produce the equipment used at its airports. **The relevant question would be whether ADC & HAS, on its own or through affiliates, transfers any "use" technology to its foreign operations relating to equipment subject to U.S. export controls.** The EAR assign a specific meaning to the term "use," which like "technology" has a very precise connotation. A company is transfering "use" technology if it is conveying the information necessary to accomplish <u>all</u> of the following tasks: operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing. Thus, if a company provides training on how to operate, install, maintain, and repair a piece of equipment, but not on how to overhaul and refurbish the equipment, then "use" technology has not been transferred.

It is important to note that all parties to an export transaction may be held responsible for compliance with the EAR – not just the exporter of record in the United States. For example, vendors and freight forwarders involved in an export transaction, as well as the foreign party receiving the export or the foreign party conducting a re-export, can be liable for violations of the EAR. BIS can issue denial orders against a party that violates the EAR (in addition to other fines and penalties), resulting in that party being blocked from sending, receiving, or participating any other way in export transactions.

2. U.S. Sanctions Laws

In addition to export control issues, ADC & HAS should be alert to sanctions issues. In contrast to export controls, which are focused on the transfers of physical items, software and technology, sanctions laws tend to be transaction-focused, and they block U.S. persons from dealing with certain countries or designated entities and individuals. Although the Commerce and State Departments have some jurisdiction over sanctions matters, the U.S. Department of the Treasury, Office of Foreign Assets Controls ("OFAC") is primarily tasked with the authority to enforce U.S. trade sanctions.

Of particular relevance to any U.S. company doing business in Latin America, directly or through its subsidiaries or affiliates, are the U.S. prohibitions on transactions with Cuba or Cuban nationals. OFAC's Cuban Assets Control Regulations (31 C.F.R. Part 515) treat foreign-incorporated subsidiaries or affiliates of U.S. companies as U.S. persons for purposes of enforcing the Cuba sanctions. Moreover, OFAC implements Counter Narcotics Trafficking Sanctions (31 C.F.R. Parts 536 and 598) and Counter Terrorism Sanctions (31 C.F.R. Parts 594-597), under which OFAC has designated and blocked thousands of individuals, organizations, and front companies, many of whom are located in Latin America. Although foreign subsidiaries or affiliates of U.S. companies are not required to comply with those particular sanctions programs, their U.S. parents or affiliates are, and they may not use foreign subsidiaries/affiliates to circumvent the compliance requirements. For that reason, many U.S.-based international companies find it helpful to implement a global compliance program in which foreign subsidiaries and affiliates are not allowed to deal with any parties that would be restricted for the U.S. company. In the event that internal personnel are not experienced in determining the level of compliance required under various sanctions laws, the company should consider engaging an outside compliance consultant to provide assistance on a periodic basis.

The following section addresses potential export compliance issues that ADC & HAS and/or its foreign subsidiaries or affiliates could encounter in their routine business activities, along with recommendations for managing those compliance risks.

B. Potential Export Compliance Issues

1. Technology Transfers

Because ADC & HAS provides technical training to its foreign affiliates on matters relating to airport operations and maintenance, the company could encounter export compliance issues in the context of U.S.-origin technology transfers. Given the low-tech nature of the work performed by ADC & HAS, however, this is not a high-risk area unless ADC & HAS performs extensive work on sophisticated airport equipment sourced from the United States (such as overhauling and refurbishing).

The technical services ADC & HAS and its affiliates provide include the following: basic maintenance of airport buildings and infrastructure (*e.g.*, buildings and roads); removal of accumulated rubber on runway, and other run-way maintenance tasks; operation of jet bridges/passenger walkways; clean-up of gasoline spills; operation and basic maintenance of

security equipment; and emergency response and firefighting services. ADC & HAS understands that the mechanical knowledge of how to perform these types of tasks is publicly available, although the specific business processes ADC & HAS uses are proprietary information.

Some of the equipment involved in these tasks is technically sophisticated and could have components subject to U.S. export controls if originally sourced from the United States, such as jet bridges, airport security devices, laptops/computers, and aircraft fire-fighting equipment. As a services provider, ADC & HAS does not "develop" or "produce" that equipment, although the company does provide training to its affiliates and their respective subsidiaries on how to operate and repair the equipment. The company would not be transferring export controlled "use" technology, however, unless ADC & HAS conveys information relating to all of the following: operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.

a. Recommendation: Technology Transfer Watch List

As a recommendation for managing the export compliance risks associated with technology transfers, it could be helpful for ADC & HAS to take an inventory of the types of training it provides to its foreign subsidiaries to determine whether any of the training relates to sophisticated and high-tech equipment that is U.S.-origin. The development of an export control watch list, as discussed further below in the section on procurement, could be useful in this exercise. If ADC & HAS transfers "use" technology to foreign nationals with respect to jet bridges, airport security devices, computers, aircraft fire-fighting equipment, and other technically sophisticated U.S. origin equipment, the company will need to determine what, if any, export control restrictions apply to that equipment (through inquiries to the product vendors and/or manufacturers) and require the vendors to obtain export licenses if necessary.

2. Procurement

In the course of performing airport operations and maintenance services, ADC & HAS affiliates are responsible for the routine procurement of equipment and materials for the airports. Almost all procurement activities take place at the local company level – ADC & HAS does not typically perform procurement services at the headquarters level in Houston. For the development and construction of new airport facilities, an ADC & HAS affiliate will hire a local engineering, procurement and construction ("EPC") contractor, who will carry out the majority of the procurement activities.

The affiliates (or their EPC contractors) procure most items in-country. That is particularly the case for construction materials and other basic items used in performing facilities maintenance, which can be sourced locally. However, some of the high-tech items used at the airport, such as aircraft fire-fighting trucks procured from OshKosh, laptops/computers, or airport security screening equipment, tend to be sourced directly from the United States through ADC & HAS corporate contracts. The company should also be alert to the possibility that some items procured from local vendors could be ultimately U.S.-origin products.

All parties to a U.S. export transaction could be held liable for export control violations, but there are various steps international companies can take to manage their exposure to export compliance risk for U.S. procurements.

a. Recommendation: Compliance Training

One common step is to provide introductory training to personnel handling or supervising procurement (at the corporate level and within the local company level), so that they are able to spot basic export control issues in their procurement activities. Many international companies also find it helpful in developing their compliance program to provide an intermediate level of training to contract managers, sales representatives, and technical leads so that they can identify potential export control issues at the beginning of a project and also advise their subordinates when issues arise.

b. Recommendation: Product Watch List

Another recommendation is to develop an export control product watch list. The list would consist of sophisticated technical equipment sourced from the United States or that might have U.S.-origin components. Some examples of items used in airport maintenance and operation could include: aircraft firefighting equipment, security devices, laptops/computers, and jet-bridges. Upon developing the list, the next step would be to reach out to the vendors or manufacturers of the equipment to request information about the export control classification number ("ECCN") and whether an export license is required for export to the destinations where ADC & HAS operates. Once the list is prepared, it should be distributed to all company and affiliate personnel involved in procurement at the corporate and local company levels, as well as personnel responsible for overseeing the EPC contractors that handle procurement. Personnel could then use the list to flag procurements raising possible export compliance issues and reach out to the designated individual(s) within the company assigned with oversight for export compliance matters. In the event that internal personnel are not experienced in determining the level of export compliance required, the company should consider engaging an outside export compliance consultant to provide assistance on a periodic basis.

c. Recommendation: Contractual Language

It is also important to develop contractual language that can be used in purchases orders and other procurement contracts, agreements with EPC contractors, and other external parties that handle procurement activities on behalf of ADC & HAS at the corporate and local company levels. Standardized language could be used in these agreements, which can be modified as needed on a case-by-case basis. The language should be clear in designating responsibilities for export compliance, for requiring the provision of complete and accurate information about ECCNs and license requirements, and indemnification for export control violations. Because ADC & HAS does not manufacture its own equipment, the vendors and manufacturers are in the best position to know what export controls apply to their products. The contractual language should protect ADC & HAS in its reliance upon the information provided by vendors and manufacturers. A draft template for export compliance language is attached to this memorandum.

3. Hand-Carried Laptops and Software

The export of U.S.-origin commercial laptop computers, pre-loaded commercial software and/or stored technical data is subject to the EAR, regardless of whether the computer is hand-carried by its owner/user or sent as a separate shipment. The procurement of computers for permanent use outside the United States is addressed in the above section dealing with procurement issues. This section addresses some unique considerations that apply to laptop computers that are hand-carried for temporary personal use outside the United States.

Virtually all commercial laptop computers come with pre-loaded software, and when bundled together, these items will together carry the ECCN of the highest-controlled item, which may require a license or license exception for export. Upon request, the computer and/or software vendors should provide ADC & HAS with the appropriate information about the ECCN of the equipment and software, as well as information about whether a license or license exception is required to export the items to a particular destination. If no license or license exception is required for a laptop with all of its pre-loaded software and technology, then the following discussion does not apply.

Laptops, software and technology that do require a license or license exception for export may qualify for the "TMP" license exception, which authorizes temporary exports of "tools of the trade" (*i.e.,* personal computers and other items used in the personal conduct of business) so long as certain requirements are met. *See* 15 C.F.R. § 740.9. The requirements that apply to use of this license exception are as follows:

- The laptop must remain under the effective control of the exporter or the exporter's employee while abroad. The laptop may not be shared with foreign nationals.

- The laptop may accompany the individual departing from the United States or may be shipped unaccompanied within one month before the individual's departure from the United States, or at any time after departure for the individual's use.

- The laptop must be returned to the United States no later than 12 months from the date of export – express authorization is required by BIS to extend the duration of the temporary export beyond that time.

- The laptop must not be exported, directly or indirectly, to Cuba, Iran, North Korea, Sudan or Syria.

4. Sanctions Compliance and Prohibited Parties Screening

As an international company with a significant portion of its operations in Latin America, ADC & HAS could encounter U.S. sanctions restrictions on dealing with certain countries (notably Cuba), individuals, and entities (particularly those designated under the anti-terrorism or counter-narcotics sanctions programs). In addition to OFAC's prohibitions on dealing with blocked persons, BIS, the State Department and several other U.S. Government agencies maintain

various lists of prohibited parties, whom ADC & HAS as a U.S. person would be restricted from dealing with.

The way most companies manage their compliance requirements under the sanctions programs and the other prohibited persons lists is to implement screening requirements for employees, partners, contractors, customers and vendors. There are consolidated screening programs available that check for BIS denied parties, OFAC blocked persons, and individuals and entities on other U.S. Government denial lists. Hughes Hubbard & Reed LLP or another compliance consultant with expertise in the area can advise as needed on various screening programs and other resources to streamline and automate that process.

5. Areas Where ADC & HAS Could Have Export Compliance Issues if It Expands Operations

During the conference call we discussed certain areas that could present export compliance concerns in the future if ADC & HAS decides to move its business in new directions. Although ADC & HAS is not currently engaged in the below activities, they are peripheral to ADC & HAS' daily business, and the company should be alert that additional export compliance risks could arise if it ventures into those areas.

a. Aircraft and Related Parts

The most obvious category of products intrinsically linked to the business of ADC & HAS are aircraft and related parts. Most aircraft, no matter where they are manufactured, have U.S.-origin components, and that content is often enough to trigger the *de minimis* requirements of the EAR. The export of aircraft and related equipment, as well as the repair and servicing of those items, can be subject to U.S. export controls.

In its current line of business, ADC & HAS does not have any direct contact with the airplanes. Rather, all operation and maintenance is provided for by the airlines that own the planes. Similarly, ADC & HAS is not involved with any activities that take place within the airplane hangars. The hangars are leased real estate and are entirely controlled by the parties that hold the leases (usually the airlines). Under the terms of its leases, ADC & HAS delivers the basic physical structure of the hangar to the airline, without making any specialized modifications to the interior. The airlines are responsible for the construction and operation of facilities within the hangars, as well as all aircraft maintenance and repair activities.

If ADC & HAS were to expand its business to include aircraft maintenance, servicing, or operations, the company would need to implement specifically-tailored compliance procedures to manage the additional risks that would be associated with these activities.

b. Air Traffic Control

Another related category potentially subject to export controls is navigation and radar equipment used in air traffic control. ADC & HAS is not presently involved in air traffic control. In all the airports operated by ADC & HAS or its affiliates, the local government provides the

necessary air traffic control services. To that end, the local government authorities own and operate any navigation and radar equipment used for air traffic control. Under its present arrangements, ADC & HAS and its affiliates are not responsible for the procurement, installation or maintenance of such equipment.

However, export control issues could arise if those arrangements change, in which case ADC & HAS would need to obtain information about the ECCN and any export licensing requirements from the product vendors or manufacturers.

c. Advance Security Services

ADC & HAS provides security services and procures related equipment. The export compliance risks associated with the company's current security activities can be managed through the recommendations set forth above relating to technology transfers and procurement. However, if ADC & HAS were to expand the range of its security services to include more advanced installation and repair of high-tech security equipment, the procurement of weapons, or the provision of training or other services to military forces, additional export compliance issues could arise.

ADC & HAS affiliates (or their EPC contractors) procure the security equipment used at the airports they manage. However, the company only performs basic maintenance on the equipment using spare parts and pre-assembled modules provided by the vendors. More extensive repairs and refurbishment are performed by the equipment distributors. Because of the technically sophisticated nature of X-ray devices and other types of security equipment, advanced levels of repairs and other activities amounting to "use" technology could be export controlled, if the equipment is U.S.-origin. If the affiliates undertake extensive refurbishment and repair activities, a recommendation for managing the export compliance risk would be to contact the vendors of the equipment to determine whether the equipment is U.S. origin. If so, the vendors and/or manufacturers should be able to provide the ECCN and obtain export licenses as required.

Security services at the airports operated by ADC & HAS are usually provided through a combination of sources, including government authorities (in some cases military forces, depending on the country), local contractors, and personnel hired directly by the ADC & HAS subsidiaries. ADC & HAS reported that it does not engage in the procurement of weapons for security officers – the government security forces and the local security subcontractors are already equipped with the weapons used in their jobs. The procurement of weapons (even if not U.S.-origin) can possibly raise export control issues under the ITAR, and further legal analysis is required if ADC & HAS determines that it will procure weapons for security personnel.

ADC & HAS does not currently provide security training or other services to government personnel. As with weapon procurement, the provision of certain types of services to foreign militaries can constitute a "defense service" regulated by the ITAR. "Defense services" can include, in part: "Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice." 22 C.F.R. § 120.9(a)(3).

Should ADC & HAS at some point become involved in providing security training to local military forces at the airports its subsidiaries manage, further legal analysis would be required to determine whether such activities fall within the scope of the ITAR.

d. Military Airbase Services

ADC & HAS does not currently provide military airbase services. In some cases, local militaries have easements and/or runway concessions at the airports managed by ADC & HAS affiliates. To that end, the military might have its own facilities at the airport, with shared airfield use. However, the military air operations are entirely separate from the civilian airport operations managed by ADC & HAS, and the company does not provide any services directly to the military. The only areas of potential overlap where ADC & HAS' services impact the military would be with regard to civilian operations, such as general airfield maintenance or fire/crash response services that ADC & HAS provides to an airport as a whole.

Should ADC & HAS decide at a future time to perform airbase management services for foreign military customers, further legal analysis would be required to determine whether there would be any export compliance/defense services issues under the ITAR.

e. Software Development

As discussed in the Overview section above, an ADC & HAS affiliate in Ecuador has been working on the development of an airport business tracking software program, which ADC & HAS is thinking about distributing for internal use company-wide. At this time there has been no U.S. involvement in the development of the software, although that could change as the software development continues to progress. Moreover, the software could become subject to U.S. export controls if it is loaded onto a U.S.-based server, or if it is brought into the United States for licensing throughout the company. Should ADC & HAS' U.S. operations become involved in contributing to the development of the software, or should ADC & HAS decide to undertake similar software development projects at the corporate level, further legal analysis would be required to determine what U.S. export control requirements could attach the software.

III. Conclusion

In summary, the areas in which ADC & HAS faces the most export compliance risk are in the categories of technology transfers and procurement of technically sophisticated equipment that is U.S.-origin. Those risks can be effectively managed through in-house compliance training, through the development of an export compliance technical service/product watch list, through obtaining export control information about those products from vendors and manufacturers, and through using strong export compliance language in purchase orders and agreements with subcontractors that handle procurement. Other areas for potential export compliance risk, if ADC & HAS and its affiliates were to expand the range of their current business, could include activities relating to aircraft servicing and operation, air traffic control, certain security activities (including advanced security equipment services, weapons procurement, or military security training), military airbase services, and development of software in the United States for global

export. Such activities would require additional legal analysis to determine the extent of the risk and to develop recommendations for managing that risk.

SAMPLE EXPORT COMPLIANCE LANGUAGE
Purchase Order Agreements

EXPORT COMPLIANCE:

Seller agrees that it will comply with the import and export laws and regulations of the United States of America, and the import and export laws of any other country, where applicable to the transaction. Specifically, Seller will provide for each item listed in the Purchase Order, as appropriate, export control classification information, and Seller is responsible for obtaining any necessary export licenses associated with the transaction.

Seller understands and acknowledges that Buyer, and its contractors and agents, will rely on the information provided by Seller. Seller will be fully responsible for the accuracy and completeness of import and export documentation provided to Buyer and other communications to Buyer undertaken in performance of this Purchase Order, including documentation required for the import or export of any materials, software, or technical data used in the production or manufacture of the Goods and of any documents prepared by Seller's employees, contractors, agents and brokers.

Seller agrees to release, defend, indemnify and hold harmless the Buyer from and against any loss, cost (including attorney fees and court costs), civil or other fines and penalties, damage or liability, arising from any violation, alleged violation, or failure to comply with, the terms of this paragraph by Seller or any person for whom Seller may be responsible.

SAMPLE EXPORT COMPLIANCE LANGUAGE
Subcontractor Agreements

EXPORT COMPLIANCE:

[Subcontractor] understands that its provision of goods, software, technical data, or services (the contract deliverables) under this Agreement, and the Company's provision of such items to [Subcontractor], may be subject to the export and re-export laws of the United States and/or the country in which the contract deliverables are provided. [Subcontractor] agrees to abide by any restrictions or conditions respecting the export, re-export, or other transfer of such items that are in effect now or are hereafter imposed by the United States Government or any other applicable governmental authority. These restrictions and conditions may include, but are not limited to, (i) restrictions and export licensing requirements governing the export, re-export, or other transfer to persons, entities, or countries of such items, and (ii) any applicable U.S. or other governmental restrictions on the export, re-export, or other transfer of such items to countries, entities and persons that are subject to U.S. or other government sanctions, embargoes, or other prohibitions.

Any violation of this Section shall be deemed a material breach of the Agreement, and [Subcontractor] shall defend, indemnify and hold Company, its officers, directors, employees and shareholders harmless from any costs, expenses, fines, penalties, or loss arising from its failure to comply with such applicable governmental laws and regulations.

[Subcontractor] further agrees that it will include this clause in its agreement with any subcontractor of any tier.