So You Want to Buy a Space Company?

*Brendan Cohen**

Abstract

In 2017, more than $3.9 billion of private capital was invested in commercial space companies. This represents, in a single year, more than half of the total amount of private investment during the preceding five years. The private space sector has also witnessed a dramatic increase in the number of investor participants. The industry continues to expand, and analysts predict that it will grow to a multi-trillion dollar industry in the next two decades. The industry is also witnessing rapidly falling launch prices – and as launch prices drop, the barrier to enter space also decreases. In addition to facilitating the expansion of existing space-based businesses, such as telecommunications and Earth observation, greater access to outer space opens the door for new entrants into fields such as space manufacturing, mining and tourism.

Almost half of all investment in space companies since the year 2000, the vast majority of which was made within the last six years, has been from venture capital ("VC") firms. VC investors seek eventually to monetize their investment by exiting through a sale of the company to a third party (usually an existing space industry player, but sometimes to another financial buyer) or through an initial public offering. Acquisitions by industry competitors are particularly common in the satellite sector, where established incumbents often look for outside innovation (for example, Terra Bella's acquisition by Planet or DigitalGlobe's acquisition by MDA). Furthermore, space activities are very costly, but benefit from economies of scale – evidenced by joint ventures between Lockheed and Boeing (United Launch Alliance) and between Airbus and Safran.

In light of the increasing frequency of mergers and acquisitions ("M&A") deal making in the space industry, this paper will examine publicly disclosed acquisition agreements governing certain prior deals in the industry in order to draw conclusions about the unique risks faced by commercial space acquirers and how they have sought to mitigate such risks. From diligence considerations to key terms of the acquisition agreements (such as the representations and warranties), this paper will provide practical insight into the most important considerations for private deals in this growing and rapidly changing industry.

* Cleary Gottlieb Steen & Hamilton LLP, United States, bcohen@cgsh.com. The opinions and views expressed herein are solely those of the author and do not necessarily represent those of Cleary Gottlieb Steen & Hamilton LLP or any of its clients.

The author wishes to thank Chris Condlin and Brinkley Rowe for their invaluable assistance in preparing this article.

I. Introduction

In June 2014, Google acquired the five-year old VC-backed satellite imaging startup Skybox for approximately $500 million. Google held the company (renamed Terra Bella) for several years, and then sold it to Planet for an undisclosed amount in April 2017. Google's foray into the space sector was by no means unique; according to Goldman Sachs, nearly $13.3 billion has been invested in space companies in the start-up phase since 2000 with a large proportion of that coming in the last 10 years.[1] In 2017 alone, estimates are that $3.9 billion of non-governmental equity investment was committed to commercial space companies.[2]

As investment has grown, innovation has followed – SpaceX has managed to decrease the cost of launches to about 60% of that of competitor incumbents (including United Launch Alliance and other pre-existing launch providers), in part due to its innovations in reusable rockets.[3] Blue Origin has similarly made strides in the field of reusable rockets and VC-funded Rocket Lab has developed a low-cost rocket designed specifically to launch small satellites to low Earth orbit.[4] This increased access to outer space provided by SpaceX and its competitors will continue to facilitate other space-based operations or services, such as space mining, on-orbit servicing, remote sensing and broadband connectivity to support the "internet of things."

In addition to investment in, and acquisition of, startup companies, there has also been consolidation among established companies within the industry. For example, Northrop Grumman acquired rocket launch and spacecraft company Orbital ATK, Inc. for $7.9 billion, a transaction that was announced on September 18, 2017 and that closed on June 6, 2018. A few years prior to Northrop Grumman's acquisition, Orbital ATK had some serious and public problems with its flagship launch system, the Antares rocket. During an October 28, 2014 mission intended to resupply the International Space Station ("ISS"), a catastrophic failure shortly after launch destroyed the rocket and its cargo.[5] The accident was the first of multiple

1 Goldman Sachs Global Investment Research, *Profiles in Innovation: Space, The Next Investment Frontier*, GOLDMAN SACHS PROFILES IN INNOVATION, Apr. 4, 2017, at 3, available at http://forum.nasaspaceflight.com/index.php?action=dlattach;topic=42684.0;attach=1449447;sess=0 [hereinafter, *Profiles in Innovation*].

2 While satellites had previously been the most funded segment within the industry, launch and landing systems became the focus of the greatest amount of investment, attracting 72% of capital deployed in 2017. *Space Investment Quarterly: Q4 2017*, SPACE ANGELS, Jan. 18, 2018, at 2, available at https://www.spaceangels.com/post/space-investment-quarterly-q42017.

3 *E.g., Profiles in Innovation, supra* note 1, at 3.

4 ROCKET LAB, https://www.rocketlabusa.com (last visited Dec. 10, 2018).

5 *E.g.,* Kenneth Chang, *Antares Rocket Explosion Leaves Questions and Dead Mosquito Eggs*, THE NEW YORK TIMES, Oct. 29, 2014, https://www.nytimes.com/

private launch failures around the same time, which also included the "rapid unscheduled disassembly" of one of SpaceX's commercial resupply rockets.[6]

Space activities are inherently risky and failures can be catastrophic, but a potential investor or acquirer in this sector must consider contingencies beyond those that are solely technical in nature. For example, government contracts represent a large proportion of the revenue available to space companies, but there is no guarantee that such funding will continue. This was probably something Northrop considered when evaluating Orbital ATK, as under its then-existing commercial resupply agreements with NASA, Orbital ATK had agreed to deliver approximately 25,000 kilograms of cargo to the ISS over 6 missions for a total cost of $1.2-1.5 billion.[7] Further, Orbital ATK's reliance on Russian-built RD-181 engines likely raised concerns due to the expiration of the federal waivers allowing Orbital to do business with Russia for ISS activities in 2020.[8] Licenses allowing for materials such as these, as well as the broader ability of these companies to conduct the launches at the heart of their business model, are often at the mercy of national and international regulatory authorities.

Rocket system and component failures, the reliance on government contracts and the significant power wielded by regulatory authorities are just a few of the risks particular to investment in a space company, and ones that Northrop Grumman must certainly have carefully analyzed before deciding to acquire Orbital ATK. The remainder of this paper will highlight certain key risks in this sector, provide some concrete examples of how these have been dealt with in other transactions and discuss possible means of mitigating issues through diligence and negotiation.

2014/10/30/science/space/explosion-leaves-questions-and-dead-mosquito-eggs-.html (last visited Dec. 10, 2018).

6 *E.g.,* Tim Fernholz, *Two Years Ago, This Rocket Exploded Trying to Reach the International Space Station. Tonight, it Flies Again*, QUARTZ, Oct. 17, 2016, https://qz.com/811420/two-years-ago-this-orbital-atk-antares-rocket-exploded-trying-to-reach-the-international-space-station-tonight-it-flies-again (last visited Dec. 10, 2018).

7 *NASA Selects Orbital ATK for New 8-Year Contract to Deliver Cargo to the International Space Station*, NORTHROP GRUMMAN, Jan. 14, 2016, https://news.northropgrumman.com/news/releases/nasa-selects-orbital-atk-for-new-8-year-contract-to-deliver-cargo-to-the-international-space-station (last visited Dec. 10, 2018).

8 *See NASA Will Pay More for Less ISS Cargo under New Commercial Contracts*, SPACE NEWS, Apr. 26, 2018, https://spacenews.com/nasa-will-pay-more-for-less-iss-cargo-under-new-commercial-contracts (last visited Dec. 10, 2018). *See also Audit of Commercial Resupply Services to the International Space Station*, NASA OFFICE OF INSPECTOR GENERAL, Apr. 26, 2018, https://oig.nasa.gov/docs/IG-18-016.pdf#page=3 (last visited Dec. 10, 2018).

II. Assessing Legal Risks in the Space Sector

A. Overview

An M&A transaction can be analogized to buying a house. First, the buyer inspects the house, for example, to make sure it has the number of bedrooms claimed, that the faucets work and that the ceiling is not cracked. The buyer asks the seller questions about the house – does it comply with the relevant building codes, are there any easements on the property or is there lead in the paint or pipes? On the assurances and representations made by the seller, the buyer makes an offer. Once the parties agree on a price, they sign the paperwork, but the buyer does not yet own the house. He may need to get a mortgage or sell his current house to have sufficient cash, or the seller may have agreed to first build a working fireplace in the living room. Any or all of these may be identified by the parties as conditions to closing the sale. Depending on what the parties have agreed, if one of these closing conditions is not met, the buyer may be permitted to walk away from the deal. Once the closing conditions are met, the buyer transfers the purchase price to the seller, and in exchange, receives the title to the house. What happens, however, if a week after the buyer moves in, he discovers that there is, in fact, lead paint covering the walls? The buyer may be able to seek legal recourse against the seller for breach of the representations that were made in the purchase agreement. The purchase of a company is no different and the various stages – the initial due diligence, the representations and covenants made by both parties, the closing conditions and the post-closing recourse available to buyer – will be discussed in the rest of this section in the context of the unique risks that are present in an acquisition or investment in a company in the space sector.

B. Due Diligence

The first, and arguably most important, stage of an acquisition or venture capital investment is the due diligence phase. It is during this process that the potential purchaser carefully examines all facets of the target's business and operations to assess the possible risks that it will later strive to mitigate. While the due diligence process will focus on more than just legal issues (typically, it will also focus on financial, accounting, tax, operational, technical and other areas of due diligence), this paper will focus primarily on the legal diligence component. While there are certain aspects of legal due diligence that will be common to all potential acquisitions regardless of the sector – such as understanding the company's corporate organization and its employee and executive compensation structure – there are certain subject areas that are particularly relevant or unique to the space sector that a potential acquirer or investor should be aware of. These subject areas include: (1) regulatory, (2) environmental, (3) insurance, (4) material contracts and (5) intellectual property and cybersecurity. This paper will also briefly address technical due diligence, which while not legal, implicates important risks in the space sector that are not present in other sectors.

The buyer will typically have diligence calls with the target, during which its representatives have a chance to ask detailed questions about each of the above-mentioned and other subject areas. The target will also provide copies of important documents – contracts, permits, lists of owned intellectual property, litigation materials, etc. This is often an iterative process, with multiple rounds of questions, presentations and document productions.

C. Representations/Warranties and Remedies

Once the key areas of risk for the target company have been identified through the due diligence process discussed above, the parties to the transaction will need to allocate these risks between the buyer and seller. In the transaction agreement, the target company makes a number of representations about each of these key areas and has the opportunity to disclose any known exceptions to such representations. Typically, the buyer will assume the risk of any known issues that have been fully disclosed by the seller during the diligence process, on the theory that the buyer has been given the chance to evaluate whether, in light of its diligence findings, to pursue the transaction or revise its price.

The role of the seller's representations is primarily to allocate the unknown risks that could arise or come to light between the signing of the deal and the closing, or in some cases, following the closing of the transaction. For example, consider a target company that is a U.S.-based launch provider, which represents that it has complied with all applicable laws. As a statement of fact, this is overly broad – it would be impossible for the target to know every law worldwide that applies to its business and to accurately interpret each and every one of those laws to be able to say with certainty that it is in compliance. Instead, the representation serves to push this unknown (and frequently unknowable) risk to the seller. If, after the signing of the transaction, this target is discovered to be exporting classified technology to a foreign country without authorization, the buyer may use this breach as a way to seek concessions from the seller, or if severe enough, may choose not to close the transaction.

In some deals, even after the closing of the transaction, the buyer may still be able to recover damages under an indemnification provision. Indemnification is a contractual right on the part of one party to recover damages from another (typically, subject to various limitations, such as deductibles and caps). In certain cases, this right to indemnification is backed by a certain portion of the purchase price that is held back from being paid to the seller at the closing to satisfy potential indemnification claims that arise after the closing.[9] However, in certain deals (for example, deals in which the target is a

9 In recent years, it has become possible for buyers to obtain insurance policies (called "representation and warranty insurance") that replicate to a certain extent, and can backstop or stand in place of, a traditional indemnity.

publicly traded company with a diffuse set of shareholders), the buyer typically has no post-closing recourse against the sellers. Similarly, venture capital investors typically do not have any remedy for a company's breach of its representations,[10] as they are understood to be making a risky investment in the growth of the company today in exchange for a chance at a large financial upside in the future – if the company is successful, so is the venture capitalist's investment.

D. Analysis of Specific Risks

The remainder of this section will discuss certain issues that a prudent buyer should examine prior to the purchase of, or investment in, a space company. This analysis is not comprehensive, and specifically avoids discussion of generalized risks common to companies of all types, but instead focuses on those that are particularly relevant in this sector.

1. Regulatory Matters

Space companies operate in highly regulated environments and have to comply with many different laws and regulations, especially when their operations are multinational. Compliance with such regulations has been identified as one of the key risks to companies operating in the aerospace and defense sectors,[11] especially since many such companies rely on governments as important customers or counterparties, whether directly or indirectly. Because of these government connections, these companies have to be even more attuned than most companies to anticorruption laws, which seek to prevent companies from making improper payments and bribes to government officials in order to obtain or retain business. In the United States, the primary regulation in this area is the Foreign Corrupt Practices Act[12] ("FCPA"), which was passed in 1977; similar regulations exist in many other countries, including the UK, China, India and Russia. In the defense sector, in particular, there have been a number of high profile cases brought against companies for violation of these laws. One such case resulted in a fine of $400 million levied by a U.S. District Court against BAE Systems in 2010, after finding that BAE Systems had willfully violated the FCPA and other regulations by making false statements regarding its compliance practices.[13] As the attorney general prosecuting the case noted at the time, "[t]he actions

10 *See, e.g.*, *Form Series A Stock Purchase Agreement*, NATIONAL VENTURE CAPITAL ASSOCIATION, Jan. 2018, at §§ 3, 4.1, 5.1, available at https://nvca.org/resources/model-legal-documents.

11 Sandipan Maiti, *Top 10 Risks in Aerospace and Defense (A&D)*, ERNST & YOUNG GLOBAL LIMITED, 2017, at 20, available at https://www.ey.com/Publication/vwLUAssets/ey-top-10-risks-in-aerospace-and-defense/%24File/ey-top-10-risks-in-a&d.pdf.

12 15 U.S.C. § 78dd-1, et seq.

13 United States v. BAE Systems PLC, Judgment in a Criminal Case (D.D.C., filed Mar. 2, 2010), Case No. 1:10-cr-00035-JDB.

of BAE Systems impeded U.S. efforts to ensure international trade is free of corruption and to maintain control over sensitive U.S. technology."[14]

The protection of sensitive technology implicates both intellectual property laws, which will be discussed in more detail below, as well as export control regulations imposed by governments in order to prevent the leakage of defense-related information to third countries. In the United States, the main export control regulations that apply to space companies are the controversial International Traffic in Arms Regulations ("ITAR"), which prohibits the export or sharing of articles or services (as well as any related technical data) that are on the U.S. Munitions List ("USML"),[15] unless the exporter receives authorization from the U.S. Department of State or fits within a specified exemption. "Spacecraft and related articles" that generally have military functions or capabilities, including launch vehicles, are on the USML (Category XV) and are regulated under ITAR. Other related technologies that are considered dual-use (that is, items having both civil, as well as military applications[16]) are controlled instead by the U.S. Department of Commerce under the Export Administration Regulations and now include certain commercial communications satellites, remote sensing satellites, planetary rovers, planetary and interplanetary probes, and in-space habitats.[17] It is also worth noting that the Committee on Foreign Investment in the United States ("CFIUS") has oversight over transactions that could result in foreign control of a U.S. business.

In response to political or industry pressures, the relevant regulations change over time, so careful due diligence into how a target company ensures continued compliance (using outside counsel, a dedicated in-house compliance function, etc.) is critical. For example, following the failures of two Chinese Long March rockets in the mid-1990s that were carrying satellites built by Hughes and Space Systems/Loral, the U.S. government added all satellites and related technology to the USML.[18] But in 2017, in response to industry lobbying, the U.S. government began to further loosen the ITAR restrictions on remote sensing satellites and spacecraft capable of

14 *BAE Systems PLC Pleads Guilty and Ordered to Pay $400 Million Criminal Fine*, U.S. DEPARTMENT OF JUSTICE, OFFICE OF PUBLIC AFFAIRS, Mar. 1, 2010, https://www.justice.gov/opa/pr/bae-systems-plc-pleads-guilty-and-ordered-pay-400-million-criminal-fine (last visited Dec. 10, 2018).

15 22 C.F.R. § 121.1.

16 *"Dual Use" and Other Types of Items Subject to the EAR*, EXPORT ADMINISTRATION REGULATIONS, at § 730.3, https://www.bis.doc.gov/index.php/documents/regulation-docs/410-part-730-general-information/file (last visited Dec. 10, 2018).

17 ECCN § 9A515.a, EXPORT ADMINISTRATION REGULATIONS, BUREAU OF INDUSTRY AND SECURITY.

18 *E.g.*, Ryan Zelnio, *A Short History of Export Control Policy*, THE SPACE REVIEW, Jan. 9, 2006, http://www.thespacereview.com/article/528/1 (last visited Dec. 10, 2018).

carrying crew.[19] As another example, the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA") was signed into U.S. law on August 13, 2018. FIRRMA expands CFIUS's jurisdiction and now requires mandatory declarations of foreign investments in certain "critical technology" industries, which include those in the space sector.[20]

Because of the highly complex web of national and international regulations, any potential acquirer must conduct careful due diligence to ensure that the target has taken the proper precautions and steps to comply with applicable laws and regulations. Any failure to do so could lead to high penalties and fines, civil investigations, termination of existing government contracts or even debarment from future government contracts, which could have catastrophic effects for a company. Finally, it is worth noting that even if a target company is in compliance with all applicable export control regulations, many in the industry see these laws (especially the U.S. regulations) as having a detrimental effect on their competitiveness in international markets due to their inability to share information with foreign persons and the fear that the government may delay or not even grant the necessary export licenses.[21] Thus, it is important for the buyer to consider its future business plans – if a company intends to acquire a U.S. satellite company with the hope of expanding operations to sell into Europe or Asia, the ITAR rules may be unduly burdensome.[22]

Further regulatory requirements (beyond ITAR and other export licensing) on companies operating in the space sector include having necessary licenses in place, in particular in connection with launch or reentry activities. This is

19 *New Rules Refine Satellite Export Controls*, U.S. DEPARTMENT OF COMMERCE, OFFICE OF SPACE COMMERCE, Jan. 10, 2017, http://www.space.commerce.gov/new-rules-refine-satellite-export-controls (last visited Dec. 10, 2018).

20 31 C.F.R. 801, Determination and Temporary Provisions Pertaining to a Pilot Program To Review Certain Transactions Involving Foreign Persons and Critical Technologies (Oct. 11, 2018).

21 *See, e.g.*, *The Nexus of the New Space Economy: 2017 Annual Report*, MAXAR TECHNOLOGIES LTD., available at http://s22.q4cdn.com/683266634/files/doc_financials/annual/Maxar-Annual-Report-2017-Final-R1[4].pdf ("Some of the [Maxar's] customers and potential customers, along with insurance underwriters and brokers, have asserted that U.S. export control laws and regulations governing disclosures to foreign persons excessively restrict their access to information about the satellite during construction and on-orbit. . . . Customers concerned over the possibility that the U.S. government may deny the export license necessary for the Company to deliver their purchased satellite to them, or the restrictions or delays imposed by the U.S. government licensing requirements, even where an export license is granted, may elect to choose a satellite that is purportedly free of [ITAR]").

22 Bijan Ganji and Dara Panahy, *ITAR Reform: A Work in Progress*, 26 THE AIR & SPACE LAWYER 7 (No. 3, 2013).

because, under Article VI of the Outer Space Treaty,[23] each State Party bears international responsibility and liability for their national activities in outer space, and they are required to authorize and supervise the activities of non-governmental entities. The Outer Space Treaty sets forth, and the Liability Convention[24] further expands on, a framework for allocating liability resulting from space activities. A launching State is strictly liable for any damage "caused by its space object on the surface of the Earth or to an aircraft in flight,"[25] and there is a fault-based liability regime for damage caused by a space object other than on the surface of the Earth.[26] Because the launching State is ultimately responsible, it is in the interest of such government to ensure that the company over which it has authority has a means of helping defray any liability that results from its activities. The launching State is any State (i) that "launches or procures the launching of a space object" or (ii) "from whose territory or facility a space object is launched."[27] Although this paper will not get into the details, there is considerable debate within the international space law community as to what exactly is a "space object" and what constitutes "damage" under the convention.[28] What is important in the acquisition or investment context is that the target company has undertaken a robust analysis to determine the applicable launching State(s) and has met all necessary licensing requirements.

In the United States, the primary agencies currently responsible for regulatory oversight and permitting of space companies include the Federal Communications Commission ("FCC") (for radio communications with satellites and spacecraft), the National Oceanic and Atmospheric Administration (for operation of private remote sensing systems) and the Federal Aviation Administration ("FAA") (for launch and reentry). As noted, each one of these agencies has different authority and oversight, but a company must have all of the proper permissions in order to legally launch or operate a spacecraft. While potential acquirers can often obtain information about the existence of permits or licenses from the websites of the relevant

23 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, opened for signature Jan. 27, 1967, 18 U.S.T. § 2410, T.I.A.S. § 6347, 610 U.N.T.S. § 205.

24 Convention on International Liability for Damage Caused by Space Objects, *opened for signature* Mar. 29, 1972, 24 U.S.T. § 2389, T.I.A.S. § 7762, 961 U.N.T.S. § 187 [hereinafter, Liability Convention]

25 *Id.* at Art. II.

26 *Id.* at Art. III.

27 *Id.* at Art. I(c).

28 *See*, *e.g.*, Elena Carpanelli & Brendan Cohen, *Interpreting "Damage Caused by Space Objects" Under the 1972 Liability Convention, in* 56 PROC. COLLOQ. L. OUTER SPACE 29 (2013).

federal agencies,[29] it is important for a potential acquirer to request copies of all relevant documents to ensure that they are still in force and cover the company's current or expected operations. Failure to do so can be costly. Satellite startup, Swarm Technologies, was recently fined $900,000 by the FCC for launching four picosatellites in January 2018, after being denied a license.[30] On this topic, it is worth noting that the U.S. Space Policy Directive-2 (signed by President Trump on May 24, 2018) is an attempt to simplify the licensing regime in the United States by February 2019.[31] As Vice President Mike Pence stated following the announcement, part of the intent of this directive is to encourage "space commerce by creating more certainty for investors and private industry."[32]

2. Environmental Matters

The manufacture, testing and launch of rockets and their payloads involves the use of hazardous substances that could give rise to environmental liability if improperly used, stored or disposed of. In addition, many newer space companies are using facilities that have, for years, been used for other purposes by older aerospace companies (e.g., SpaceX's Hawthorne headquarters and factory was once used by Northrop Grumman to build 747s[33]). Years of rocket fabrication and testing can take their toll on the local environment around a particular facility and lead to large historic environmental liabilities.[34] Under the U.S. Comprehensive Environmental

29 *E.g.*, *Active Licenses*, FEDERAL AVIATION ADMINISTRATION, https://www.faa.gov/data_research/commercial_space_data/licenses; *Universal Licensing System*, FEDERAL COMMUNICATIONS COMMISSION, http://wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp; and *Commercial Remote Sensing Regulatory Affairs; Licensing*, NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION, https://www.nesdis.noaa.gov/CRSRA/licenseHome.html (each last visited Dec. 10, 2018).

30 *See, e.g.*, Caleb Henry, *FCC fines Swarm $900,000 for unauthorized smallsat launch*, SPACENEWS, Dec. 20, 2018, https://spacenews.com/fcc-fines-swarm-900000-for-unauthorized-smallsat-launch/ (last visited Dec. 21, 2018).

31 Marcia Smith, *Text of President Trump's Space Policy Directive 2, May 24, 2018*, May 24, 2018, SPACEPOLICYONLINE.COM, https://spacepolicyonline.com/news/text-of-president-trumps-space-policy-directive-2-may-24-2018 (last visited Dec. 10, 2018).

32 *Statement from Vice President Mike Pence on the President's Signing of Space Policy Directive-2*, THE WHITE HOUSE, May 24, 2018, https://www.whitehouse.gov/briefings-statements/statement-vice-president-mike-pence-presidents-signing-space-policy-directive-2 (last visited Dec. 10, 2018).

33 *E.g.*, Michael Belfiore, *Inside SpaceX: We Visit the Company's California Headquarters*, POPULAR MECHANICS, Jan. 20, 2012, https://www.popularmechanics.com/space/rockets/g768/inside-spacex-we-visit-the-companys-california-headquarters (last visited Dec. 10, 2018).

34 *See*, *e.g.*, In the Matter of: Northrop Grumman Systems Corporation Corrective Action Consent Agreement, STATE OF CALIFORNIA ENVIRONMENTAL PROTECTION AGENCY DEPARTMENT OF TOXIC SUBSTANCES CONTROL, Jun. 30, 2003, available at https://www.dtsc.ca.gov/HazardousWaste/Projects/upload/NorthropGrumman_ENF_

Response, Compensation and Liability Act, in the event of environmental contamination at a site, each potentially responsible party is both strictly liable (i.e., without regard to negligence or failure to observe a standard of conduct) and jointly and severally liable (i.e., liable for the full amount of damages, regardless of whether there are other responsible parties) for the entire cleanup of the site.[35] Thus, unless careful due diligence is conducted, a buyer could unintentionally inherit an unexpectedly large contingent liability. In addition, many government contracts have strict provisions regarding compliance with all federal, state, and local environmental laws, including obtaining environmental permits. Often, a government contractor is also liable for any environmental contamination or noncompliance by its subcontractors. Space companies may require access to U.S. Air Force or NASA facilities for launch or testing, and in such contracts, the applicable government agency often receives broad rights to inspect all facilities and records to ensure the contractor's compliance. Any violation of a term or condition of an environmental permit or license may give the government a right to terminate the company's access. Violations of certain environmental laws can result in criminal convictions, for example, under the Clean Water Act or Clean Air Act,[36] and such a conviction could lead to the mandatory debarment of the company and a prohibition on future participation in federal government contracts until the issue is remediated. Thus, a company's violations of the environmental compliance requirements in these contracts could result in anything from costly interruptions to its operations, to a complete bar on transacting with the government, depending on the severity of the violation.

3. Insurance

Space activities are extremely risky and can result in significant liability. The operation of a launch vehicle, in particular, can end in a catastrophic failure that results in property damage (including to the launch vehicle itself, its payload, the launch facilities or third-party property) and personal injury (to those on board or unrelated third parties). In-orbit activities can also result in

CACA.pdf (describing release of hazardous waste materials into the groundwater at an East Hawthorne, California rocket production facility, owned by Northrop Grumman at the time).

35 *See*, *e.g.*, *2016 Annual Report*, AEROJET ROCKETDYNE HOLDINGS, INC., at 15-16, available at http://ir.aerojetrocketdyne.com/static-files/de144a19-4041-41a1-9e14-429978f1abcd.

36 *See*, *e.g.*, Environmental Assessment for Issuing a Reentry License to SpaceX for Landing the Dragon Spacecraft in the Gulf of Mexico, FEDERAL AVIATION ADMINISTRATION, Aug. 14, 2018, available at https://www.faa.gov/about/office_org/headquarters_offices/ast/environmental/nepa_docs/review/launch/media/Final_EA_and_FONSI_SpaceX_Dragon_Gulf_Landing.pdf (describing the FAA's process for assessing potential Clean Air Act Violations as part of assessments related to SpaceX's license for space launches over the Gulf of Mexico).

damage to another space object or to people or property on Earth following an uncontrolled reentry.

Space companies frequently obtain insurance to cover a variety of risks associated with their operations. It is common for commercial satellite operators to obtain property insurance for loss or damage of payloads during launch and for the duration of the first year in orbit,[37] and in fact, in the United States, procurement of adequate insurance is one of the requirements in order to get a commercial launch license.[38] A company seeking a license must obtain an insurance policy to cover potential liabilities for claims by a third party for personal injury or property damage resulting from the launch activity. The policy must cover the company, the U.S. government, and each of its and their employees and contractors for an amount up to the FAA's determination of maximum probable loss, but which will not exceed $500 million or the maximum liability insurance available on the world market at reasonable cost. Beyond that, up to a total of $1.5 billion (plus inflation[39]), the U.S. government will indemnify the launch licensee for any successful claims (including reasonable litigation or settlement expenses).[40] For amounts exceeding what the government will indemnify, the launch company must bear any additional liability or seek optional supplemental third-party insurance.

Another requirement for a launch license under U.S. law is that launch providers and their payload customers enter into cross-waivers of liability under which each party agrees not to sue the other party for any damage or losses sustained resulting from an activity carried out under the applicable license.[41] Because the parties to the launch assume the risk for any damage they suffer in connection with the licensed activities, a payload provider may have no recourse against a launch services provider, even if such provider were negligent in providing its services. For these reasons, making sure that a target company has adequate insurance to cover the cost of replacing a satellite or other payload in the event of a failure is crucial.

37 *See* Pamela L. Meredith, *Commercial Space Transportation: Liability and Insurance*, AIR TRANSPORT, AIR & SPACE LAW AND REGULATION, Abu Dhabi, Apr. 2009.

38 51 U.S.C. § 50914; 14 C.F.R. § 440.9.

39 This was estimated to be about $3.06 billion adjusted for inflation to fiscal year 2016. *See Report to Congressional Committees: Commercial Space Launch Insurance: Views Differ on Need for Change to Insurance Approach but Clarification is Needed*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, at 10, Nov. 2016, available at https://www.gao.gov/assets/690/681200.pdf.

40 51 U.S.C. § 50915.

41 51 U.S.C. § 50914(b). *See also* Orbcomm Inc., Annual Report (Form 10-K/A) (Apr. 30, 2013), at Exhibit 10.2 (Launch Services Agreement), Art. 8, available at https://www.sec.gov/Archives/edgar/data/1361983/000119312513112208/d468141dex102.htm.

In the context of an acquisition or an investment, it is important to understand both (a) whether the target company has adequate insurance in place (and, if not, to prepare to put such policies in place following the closing) and (b) the insurance requirements that the company currently faces or will face when it applies for any applicable licenses and what rights to recover may have been waived.

4. Material Contracts

Another important area of diligence for an acquirer to undertake is a careful review of the target company's material contracts. These contracts can include supply agreements for the purchase of components, vendor contracts for the provision of certain necessary services, lease agreements for office space, ground stations or launch sites, customer contracts with the target's key customers or research and development or intellectual property license agreements through which the target company acquires or receives rights to certain important technology. As noted above, the government is often involved as a direct or indirect recipient of services from many companies operating in the space sector, and contracting with governmental agencies has intricacies not found in contracting with commercial third parties. In the United States, procurement contracts that are governed by the Federal Acquisition Regulation ("FAR"), give governmental agencies significant rights vis-à-vis their contractual counterparties. While the consequences of reliance on government contracts will likely not be a reason to walk away from a deal, it is nonetheless important for a buyer, especially one not already in this industry (for example, a venture capital investor) to understand not only the potential risks, but also the rights that the government has.

The government has broad rights to terminate contracts for convenience at any time, and the contractor would only be entitled to recover costs incurred up to the point of termination, a reasonable profit on such incurred costs and any settlement expenses, but not its lost profits on the terminated work. In addition, pursuant to the Anti-Deficiency Act, the U.S. government cannot order any goods or services unless it receives funding from Congress. Since the Congress may choose to cease a program at any time, there is a risk that the target company could lose significant expected revenues. The risks of debarment as a result of failure to abide by anticorruption and other similar regulations have been discussed above, but it bears reiterating that debarment from participating in future government contracting could have devastating effects on a company operating in this industry.

With respect to the other (non-government) contracts of a counterparty, it is particularly important to review these to ensure that they will continue in force following the consummation of the acquisition of the target company or, alternatively, whether they will require consent from the counterparty in connection with the transaction. It is not uncommon for agreements such as

inbound intellectual property license agreements to be personal to the target. The counterparty may not want one of its competitors to have access to certain technology, and will therefore seek to ensure that if the licensee is acquired or the relevant business unit is sold, the license agreement terminates. In such situations, the parties will need to seek the consent of the counterparty.

5. Intellectual Property and Cybersecurity

Two other areas in which it is particularly important to conduct due diligence are intellectual property ("IP") and cybersecurity. At a high level, a buyer should review and understand the target's IP portfolio and strategy, ensure that the target has taken commercially reasonable steps to protect its trade secrets, ask about any pending or threatened disputes with respect to IP, and, given the importance of government contracts, understand the government's rights to any IP of the target. The buyer should also ask about the company's cybersecurity practices and any obligations imposed by law or by contract. These will be discussed in more detail in this section.

i. Intellectual Property

Part of the underlying value proposition for the acquisition of an aerospace company could be based on its technology, which is protected by a variety of IP rights, including patents, trade secrets and copyrights. Every company will have a different IP portfolio management strategy that includes whether to file for patents on new inventions or to keep such inventions as trade secrets. SpaceX, for example, has essentially no patents. This is a conscious decision on the part of CEO Elon Musk, who explained in an interview that "[SpaceX's] primary long-term competition is in China—if [SpaceX] published patents, it would be farcical, because the Chinese would just use them as a recipe book."[42] As of this writing, competitor Blue Origin holds approximately 20 published U.S. patents, according to public U.S. Patent and Trademark Office Records. Unlike patents, which must be disclosed to the world in exchange for a 20-year monopoly, trade secrets are protected from unauthorized use or disclosure for so long as they remain secret and provide the owner with an economic advantage because of such secrecy. Trade secrets may protect manufacturing processes, chemical formulae or even software source code. Source code may also be protected by copyright law.

Regardless of the IP strategy that the company takes, because of the importance of IP to most companies in this sector, it is critical to ensure that the company owns any IP developed by its employees and contractors, rather than such IP remaining with its creators. The diligence process should include a review of the target company's employment or consulting contracts (at least

42 Chris Anderson, *Elon Musk's Mission to Mars*, WIRED, Oct. 21, 2012, https://www.wired.com/2012/10/ff-elon-musk-qa/all (last visited Dec. 10, 2018).

the company's form agreement) to make sure that employees and consultants clearly (a) assign to the company all IP created in the course of employment, (b) agree to maintain the confidentiality of all trade secrets they develop or learn on the job and (c) covenant that they have not taken any trade secrets from their former employer. Trade secret misappropriation can cost companies significant amounts of money, both in terms of loss of competitive advantage and legal fees. A highly publicized case in this sector from 2009 concerned a former Boeing engineer who was convicted of stealing space shuttle-related trade secrets for the benefit of the government of China.[43] In another case that was decided more recently, a NASA supplier, Advanced Fluid Systems Inc., was awarded a $3.1 million judgment against a former employee who was found to have stolen thousands of documents related to hydraulic systems used to retract rocket platforms after liftoff and provided them to a competitor, which then usurped business from Orbital Sciences Corp. (now Orbital ATK).[44]

In addition to trade secret misappropriation litigation, there is a risk that the target company may be infringing other third-party IP – that is, using that IP without authorization. Because patent infringement does not require knowledge of the existing patent or any volition on the part of the alleged infringer, it is difficult for a company to determine its patent infringement risk. Most savvy companies will conduct "freedom to operate" or other clearance searches that try to determine whether there are any third party patents that may be infringed by a new product or service that the company plans to introduce. Proactively attempting to identify (and design around) known patents could save a company significant amounts of money in the future. Thus, any potential buyer or investor should understand the steps the company takes to protect itself and must be aware of any existing or threatened IP disputes. The representations a target company makes relating to the unknown risk of IP infringement is often one of the most hotly contested part of the IP negotiations.

Generally, when IP is developed using government funds or pursuant to a government contract, the government retains certain rights to such IP. A company may retain ownership of certain inventions developed with government funds or pursuant to a government contract, provided it properly adheres to the specified process and timeframe for disclosing and electing to retain title thereto. The company may still lose ownership if it does not prosecute the patent diligently, which may limit the company's freedom to choose to protect a retained invention as a trade secret. Even companies that successfully elect to retain ownership must grant the government a license to practice the invention. U.S. law also grants the government certain "march-in

43 United States v. Chung (C.D. Cal, Jul. 16, 2009), SACR 08-00024-CJC.

44 Advanced Fluid Systems Inc. v. Huber et al. (M.D. Pa., filed Dec. 24, 2013), Case No. 1:13-cv-03087.

rights," which may allow the government to force the owner of a retained invention to grant a license on reasonable terms to a third party (even a competitor) under certain circumstances, for example, failure to conduct manufacturing operations primarily in the United States. For data and computer software, the government receives certain non-exclusive license rights ("unlimited," "restricted," "limited" or "government purpose" rights) based on the type of data or software in question and the type of government support provided. A company must also mark proprietary data delivered to the government with appropriate legends pursuant to government regulations in order to preserve its rights, so it is important to ask questions of the target company to ensure that it has done so.

ii. Cybersecurity

Cyberattacks are a growing threat to all companies. A common trope is that there are only two types of companies: those that know that they have been hacked and those that do not know. Because of this increasing risk, an important aspect of the diligence process is to understand what precautions the target company has taken to protect its information technology systems against unauthorized breaches or intrusions and to understand what its obligations are in the inevitable event of an incident.

Most companies in this sector are handling some form of controlled information[45] and many may be contractors or subcontractors of government agencies, including the U.S. Department of Defense ("DoD"). In order to preserve the security of controlled unclassified information, the DoD requires compliance with certain standards for security[46] that are prescribed by the National Institute of Standards and Technology.[47] These regulations require that the contractor or subcontractor put into place certain security-related mechanisms. These include implementing access controls to controlled information, undertaking security awareness training for employees, performing self-tests or assessments related to information technology vulnerabilities and having an incident response plan in place (often with an obligation to report any cyber incident within 72 hours of discovery). Even if the target company is not subject to more stringent defense-related obligations, its contractual counterparties may require certain of these obligations, in particular, notification of a breach, so as to ensure that their

45 *See, e.g.*, *New DFARS Regulations = New Standard for Cybersecurity*, AMERICAN INSTITUTE OF AERONAUTICS AND ASTRONAUTICS, https://www.aiaa.org/januaryprotocol (last visited Dec. 10, 2018).

46 DFARS § 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting).

47 *See, e.g.*, Ron Ross, Kelley Dempsey, Patrick Viscuso, Mark Riddle and Gary Guissanie, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST § 800-171 Rev. 1 (Jun. 7, 2018).

own confidential or proprietary information (including trade secrets) is protected.

Like technical due diligence, which is discussed in the next section, the analysis of the target company's systems and processes will likely not be the job of the lawyer, but asking the right questions and ensuring that the company has policies and procedures in place to address its legal or contractual obligations is important. The target should certainly share information about any known breaches or attacks that have, or could have, resulted in the theft or unauthorized use of sensitive data or information. It is also important to know whether there have been any notifications provided to a government, regulator or any third party about such an incident. If the target conducts audits or penetration tests, the buyer should review these assessments and understand the weaknesses and any remediation efforts undertaken by the company. Finally, as with other types of risk, the buyer should make sure to get strong representations on these issues from the seller.[48]

6. Technical Due Diligence

In addition to legal due diligence, a buyer should conduct technical due diligence of the target's products, services and other assets to ensure that they function and operate as expected. While the technical review is typically outside the scope of the lawyer's diligence efforts, negotiating protections in the merger agreement for the buyer in the event that such assets do not perform as the target company has described is a key role of the deal lawyer.

The buyer will typically request that the target company make a number of representations about its assets and disclose any known issues or deficiencies. One form that this representation takes is a statement by the seller about the sufficiency of the company's assets – that is, that the company owns or has a right to use all of the assets, properties and rights that it needs to operate its business.[49] The representation is a general one and covers all kinds of assets and rights, from the lease of the property for the corporate headquarters to the desks for employees to the intellectual property.

48 *See, e.g.*, DigitalGlobe, Inc., Current Report (Form 8-K) (Jul. 23, 2012), at Exhibit 2.1 (AGREEMENT AND PLAN OF MERGER, Dated as of Jul. 22, 2012, by and among DigitalGlobe, Inc., 20/20 Acquisition Sub, Inc., WorldView, LLC, and GeoEye, Inc.), § 3.12(g), available at https://www.sec.gov/Archives/edgar/data/1208208/000114420412040518/v319217_ex2-1.htm [hereinafter DigitalGlobe 8-K].

49 *See, e.g.*, Northrop Grumman Corp., Current Report (Form 8-K) (Aug. 17, 2018), at Exhibit 2.1 (AGREEMENT AND PLAN OF MERGER Among NORTHROP GRUMMAN CORPORATION NEPTUNE MERGER, INC. and ORBITAL ATK, INC., Dated as of Sep. 17, 2017), § 3.01(n), available at https://www.sec.gov/Archives/edgar/data/866121/000110465917057495/a17-22167_1ex2d1.htm.

In addition, where there are particularly material pieces of equipment, such as satellites or launch vehicles, the buyer may demand that the seller disclose these and list all known anomalies or incidents with such assets. In the purchase agreement governing MDA's 2017 purchase of DigitalGlobe, for example, DigitalGlobe was required to provide a schedule, which included for each of DigitalGlobe's satellites, (i) the launch date, (ii) the best ground resolution, (iii) the annual collection capacity, (iv) the orbital altitude, (v) the expected end of depreciable life and (vi) the net book value. DigitalGlobe further represented that it had all rights necessary to operate each such satellite, and that there were no material abnormalities in, diminutions of capacity of, degradation of, damage to, loss of, or destruction of, each such satellite.[50]

III. Conclusion

Investment in space has grown dramatically in the last several years and the trend does not appear to be slowing down. Seasoned investors or acquirers may have some experience investing in startup companies, but as described in this paper, the space sector poses unique challenges and risk. It is one that requires significant upfront investment and is fraught with technical challenges that must be overcome. Adding a complex regulatory regime and the potential for large contingent liabilities creates a landscape that could be difficult for the would-be investor or acquirer to navigate. As discussed, however, careful due diligence and thoughtful contractual protections can help mitigate this exposure to a certain degree. This paper has addressed certain of the risks a buyer should be aware of in the context of an acquisition of, or investment in, a space company, but as every transaction is unique, retaining competent counsel and technical advisers is key.

50 *See* DigitalGlobe 8-K, *supra* note 48, at § 3.17(b).