*Testimony of Richard DalBello before the Science and Space Subcommittee of the U.S. Senate Committee on Commerce, Science and Transportation, "**Assessing the Risks, Impacts and Solutions for Space Threats**."*

March 20, 2013, 10:00 AM.

Commercial Satellite Communications: Assessing the Risks, Impacts and Solutions for Space Threats.

Good morning. I am Richard DalBello, Vice President of Government Affairs for Intelsat.

It is a pleasure to be here today to discuss the "Risks, Impacts, and Solutions for Space Threats" as they pertain to the commercial satellite industry. As requested, I will also comment on the state of the current collaboration between industry and government on these topics and offer some ideas on how to improve the planning and cooperation between the U.S. government and the industry.

Intelsat is the world's leading provider of satellite services. With almost 50 years of service and over 50 satellites in orbit, we are familiar with the complex challenges of this industry. As a global fleet operator, our concerns go beyond the operation of individual satellites but are, instead, focused on the maintenance of a highly sophisticated global fleet of satellites and our IntelsatOne terrestrial network, providing a multiplicity of services to large media, corporate, and government customers.

Continuity of service is one of the highest priorities of our commercial and government customers. Large media companies, broadcasters, global corporate networks, and government

users must feel that our satellite services are dependable and that their critical services will not be interrupted. Thankfully, today's satellites are highly reliable and they often outlive their notional 15-year lifetimes. Of course, anomalies can occur and satellites must be replaced at the end of their useful lives. Maintaining a fleet of over 50 satellites means that we are launching several replacement satellites each year. This raises two other significant topics: the importance of a vibrant, domestic launch industry and the relevance of investments in next-generation technologies to allow the refueling and repair of satellites on orbit. Although these topics are beyond the scope of this hearing, they have a significant impact on our country's current and future ability to respond to space threats.

Increased Reliance on Satellite Communications

Over the last several decades, the US economy and the Federal Government have both grown increasingly reliant on the commercial satellite communications industry. Today, such vital activities as television broadcasts, the Internet, oil and gas exploration and production, financial transactions and agricultural production all depend, in part, on the ability to communicate by satellite.

Our economy now depends on the ability to create and instantly distribute vast amounts of information around the world. Space-based communications platforms have become vital to the day-to-day linking of national and global economics, the prediction of weather, the navigation of virtually all forms of transportation, the operation of power grids and the completion of local and global financial transactions. In remote parts of the globe, satellites provide the only link to more populated areas. A sudden loss of satellite communications would cause significant economic disruption.

The commercial satellite industry also plays a critical role in supporting government operations, including national security and emergency preparedness missions. The commercial industry supplied the majority of the satellite communications used for military operations in Afghanistan and Iraq and continues today to provide nearly all beyond-line-of-sight communications for our unmanned aerial vehicle (UAV) fleets.

Commercial Satellite Vulnerabilities and the 2009 NSTAC Report

In 2008, Intelsat participated in a review by the President's National Security Telecommunications Advisory Committee (NSTAC) to identify both physical and cyber security threats facing the commercial satellite industry, mitigation measures employed to combat such threats, and initiatives to develop a standard security framework among satellite operators to enhance national security. [1] The report was published in 2009, but its major conclusions are still relevant today.

Among the NSTAC Report's conclusions were:

- *Radio Frequency Interference (RFI)* -- Radio frequency interference represents a significant and growing threat to satellite services, yet Government and industry do not collaborate systematically to share information regarding the detection, characterization, geolocation[2], and mitigation of interference. The Government engages with industry only when a Government service is affected instead of working collaboratively with industry to identify best practices and establish shared situational awareness and mitigation approaches.

[1] NSTAC. (2009). *NSTAC Report to the President on Commercial Satellite Communications Mission Assurance*.
[2] Geolocation is a technique that allows satellite operators to rapidly identify the location of an interfering signal by using advanced signal processing techniques coupled with other known information.

- *Cyber security* -- The terrestrial components of satellite networks contain many of the same subsystems found in other communications networks. As a result, satellite and terrestrial networks share similar cyber vulnerabilities and mitigation measures. However, because satellites must be controlled remotely from Earth, satellite operators take special care to mitigate two risks: (1) remote introduction of a false spacecraft command; and (2) a malicious third party preventing the spacecraft from executing authorized commands or interfering with satellite telemetry reception. Consistent with Government policy, most satellite companies use the National Security Agency-approved satellite command uplink encryption for satellites supporting U.S. Government services.

- *Space Traffic Control* - While an accidental collision between space debris and a satellite is unlikely, collisions do occur, can be catastrophic, and can cause permanent damage. The February 2009 collision of an Iridium communications satellite and a defunct Russian Cosmos satellite provides one example. Every such collision produces additional debris that remains in the space environment, often for years, and poses an ongoing threat to other spacecraft. Preventing collisions is of paramount importance. The NSTAC found that, today, the Department of Defense (DoD) shares only limited space situational awareness information with private industry. However, promising initiatives such as industry's Space Data Association should promote better location sharing, maneuver coordination, and collision avoidance.

- *Protection of Terrestrial Infrastructure* – Satellites are far less likely than terrestrial facilities to be the target of a successful physical attack due to their location in space. The NSTAC found that satellite operators use redundant and geographically diverse

facilities to protect terrestrial infrastructure from man-made and natural threats to ensure continuity of critical satellite network functions. Ground stations are connected by redundant, path-diverse, cryptographically secured communications links and employ preventative measures such as buffer zones and robust security systems to protect from attack. Further, operators maintain personnel security procedures, including background checks, employee badges, logged entry and exit, and on-site security guards, as part of their best-practice security efforts.

- *Collaborative Forums for Government/Industry Dialogue* -- The NSTAC report noted, with approval, the creation by DoD of the Mission Assurance Working Group (MAWG) to encourage a constructive and collaborative relationship between DoD and the satellite industry, including at the classified level. The MAWG had undertaken a variety of issues including enhancing compliance of commercial services with DoD mission assurance requirements, increasing mission assurance through modifications and improvements to communication architectures, and suggesting new or revised capabilities for commercial service acquisitions.[3]

- *Long Term Planning* – Satellite operators make every effort to replace existing satellites with updated or enhanced systems to meet both future commercial and Government user requirements. However, the Government does not engage with industry in planning for its long-term communications needs. As a result, the Government relies on the "spot market" to meet most long-term service needs and risks a potential shortfall in commercial satellite availability when critical needs arise.

[3] Since the publication of the NSTAC report, the MAWG has been disbanded. Discussions are underway between DoD and industry to replicate some of the functions of the MAWG but, to date, no formal structure has been established.

- *Space Weapons* -- Due to the technological availability and/or cost of mitigation, the commercial satellite industry does not mitigate the risk of nuclear detonations or space weapons.

Space Data Association – Industry Collaboration on Safety of Flight[4]

Since the launch of Sputnik in 1957, governments and commercial companies have placed thousands of satellites in orbit around the Earth. Most of them have long since burned up reentering the atmosphere or disintegrated into space debris. Today, there are still more than 16,000 active satellites and debris objects in the public catalog of tracked objects.

The region of space near Earth in which satellites orbit is so large – extending out 22,200 miles for commercial satellites – that one might believe a collision of orbiting spacecraft would be impossible. However, just four years ago, a satellite operated by Iridium Communications for the company's global communication network collided with an uncontrolled Russian spacecraft that had been out of service since 1995. The collision, 490 miles above Siberia, produced over 2,000 pieces of debris larger than 10 centimeters (3.9 inches) in diameter, each one large enough to destroy any orbiting satellite in its path.[5]

To avoid collisions in the increasingly crowded orbital arcs, agencies and companies operating satellites have informally shared position and orbit data for many years. One problem with this informal information sharing is that satellite operators don't use the same standard to represent the position of a satellite in orbit or an object in space. Many different types of software are used

[4] Some of the material in this section was previously published. See: DalBello, Richard. (2011). Managing Risks In Space. Federation of American Scientists. Retrieved from https://www.fas.org/pubs/pir/2011winter/2011Winter-ManagngRiskinSpace.pdf.
[5] NASA Orbital Debris Quarterly News, July 2011.

to track and maneuver satellites and the data is stored in a variety of formats. So even operators who wish to share data can't rely on a single, agreed-upon protocol for sharing information. As a result, operators sharing information must maintain redundant file transfer protocols and tools to convert and reformat data so that it is consistent with their own software systems to compute close approaches. As the number of satellite operators increases, the problem of maintaining space situational awareness grows more complex. And the smallest operators may not be able to afford, or have the technicians, to participate in the data sharing process.

Recently, the world's leading commercial satellite operators formed the Space Data Association (SDA) to formalize the process of exchanging information and to deal with the overall data compatibility problem. One way to minimize risk in space is for all operators to share what they know about the movement and position of their own satellites in a way that all other companies can use. While this sounds like common sense, governments and commercial companies around the world have each historically acted predominantly on their own in launching and monitoring satellites. Agencies and companies coordinate frequency allocation and orbital slots prior to launch, but once a satellite is in orbit, data about the movement of commercial satellites was shared only informally until the establishment of the SDA. Information about the operation and location of many military and intelligence satellites is still shrouded in secrecy.

The most critical times to share data about satellites are when a new satellite is being placed in orbit or an existing satellite is being shifted from one orbital slot to another. A typical communications satellite is as big and heavy as a loaded semi-trailer, and though it appears fixed above the Earth, it is actually traveling thousands of kilometers per hour. Putting a satellite into an orbital slot or moving it to another position above Earth without disturbing any of the

other 250+ commercial communications satellites in the GEO[6] plane, as Intelsat routinely does, is a very delicate operation. Yet this process is managed entirely by commercial operators using informal, de facto rules developed through experience and implemented by consensus.

The formation of the SDA is a major step toward creating a voluntary "space traffic control" system for space. The SDA is an interactive repository for satellite orbit, maneuver, and payload frequency information.[7] The SDA's principal goal is to promote safe space operations by encouraging coordination and communication among its operator participants. Through the SDA's Space Data Center, the satellite operators maintain the most accurate information available on their fleets; augment existing government-supplied data with precise orbit data and maneuver plans; and retrieve information from other member operators when necessary. As a result, the data center:

- *Enhances Safety of Flight.* The SDA aims to preserve the space environment by rapidly and automatically sharing information about the positions of satellites in space.

- *Reduces Radio Frequency Interference.* Radio frequency interference – both intentional and accidental – is the number one operational problem facing communication satellite companies today. By sharing the precise location of commercial satellites and the configuration of their payloads, operators can more rapidly find and address interference sources.

[6] Most commercial and military satellites operate in one of two orbit planes. The first, low-Earth orbit (LEO), is between 160 and 2,000 meters (100-1,240 miles) above Earth's surface. The other, geostationary Earth orbit (GEO), is a circular orbit 35,786 kilometers (22,236 miles) above the equator.
[7] See: www.space-data.org.

- *Simplifies Communication in a Crisis.* Before creation of the SDA, the world's satellite operators had no authoritative index of contact information for engineers actually controlling another company's satellites. Although there was always a great deal of informal communication, the SDA has standardized and automated the information necessary to communicate between technicians in operations centers during a crisis.

Because of the proprietary nature of the operational data, the SDA has been designed to protect information and prevent participants from using for commercial purposes the data supplied by other operators. The participants of the SDA contribute operational data through a secure interface on a daily basis and can access data related only to the operation of their own satellites. For example, an operator who only has satellites covering Latin America cannot access data from other parts of the globe.

So far, the SDA has 21 contributing operators and maintains precise position information on 267 satellites in GEO, and another 90 satellites in LEO. Additionally, both NASA and NOAA joined the SDA in 2012. The greater the participation of the SDA, the more comprehensive the data and the resulting analysis will be. As new satellite operators continue to join the SDA, the data center will continually improve its reliability in all satellite arcs and develop into a truly global and comprehensive database for space situational awareness.

Several years ago, the U.S. government began providing the public, including satellite operators, with satellite position data gathered, using radars and sensors, by the U.S. Strategic Command (USSTRATCOM). The position information provided initially for close-approach monitoring, called two-line element (TLE) data, had several drawbacks. First, there was no fixed standard for TLE interpretation. Second, TLE data did not have the required accuracy for

credible collision detection. Recently, USSTRATCOM developed a procedure for providing satellite operators with more comprehensive information in the form of conjunction summary messages (CSMs). These CSMs are used to warn operators whose satellites have been identified by STRATCOM as closely approaching another space object.[8] These CSMs contain vector and covariance information computed from other data, making them more accurate than TLEs.

However, recent studies funded by Intelsat and SES have concluded that to ensure the highest level of accuracy, it would be beneficial for USSTRATCOM to incorporate data from routine satellite maneuvers. The SDA has offered to augment the global data maintained by USSTRATCOM with more precise operator-generated data to improve the accuracy of conjunction monitoring. The SDA could also provide a standardized method and focal point for operators to share information and facilitate communications between satellite operators and governments interested in making available timely space object catalogues. Hopefully, with the passage of time, the U.S. and other governments will be able to fully capitalize on this industry-sponsored and funded initiative. Solving the problem of government/industry data sharing and the role of the SDA should be a key objective of future international discussions on this topic.

Another major risk to operators is the proliferation of orbital debris from rocket stages, defunct satellites, equipment lost by astronauts and the fragments left from explosions and collisions of satellites. For example, Vanguard 1, launched by the United States in 1958, is expected to remain in orbit at least another 200 years before slowly burning up as it drifts down into the atmosphere.[9] The debris problem is most severe in low-earth orbit (LEO), where the majority of satellites used for communications and remote sensing operate. Because these satellites are

[8] Statement of Major Duane Bird, USAF, US Strategic Command to *AMOS Conference*, September 2010.
[9] NASA's National Space Science Data Center.

not geostationary, multiple satellites, rather than a single satellite, are required to provide continuous coverage of any given area.

While governments were the first to send satellites to near-Earth space, commercial enterprises and consumer services will be the primary users of the orbital arcs in the 21st century and, hopefully, beyond. Consequently, governments and companies operating spacecraft need to take a more collaborative approach to enhancing the safety and efficacy of the space environment. The Space Data Association is the major step on this path, and that step should be followed by firm actions of governments and all space users to create an international framework that assures the preservation of this valuable resource.

Radio Frequency Interference

Radio frequency interference (RFI) is a serious problem that costs the satellite industry millions of dollars each year. The users of satellite services routinely state that RFI is the single most important issue relative to their use of satellite services.[10] RFI disrupts television signals, data transmissions and other customer services, requiring significant operator resources and hindering business growth. Interference has a financial impact as well to satellite operators and users. When there is interference on a satellite, there is revenue lost due to the reduction of available bandwidth and power capacity. Expenses are increased, ranging from the purchase of interference monitoring or geolocation equipment to hiring and dedicating personnel to interference mitigation.

[10] Intelsat. (2012). *Carrier ID Wins a Gold Medal at the 2012 Summer Olympics.* [Blog]. Retrieved from http://www.intelsatgeneral.com/blog/carrier-id-wins-gold-medal-2012-summer-olympics.

Intelsat has played a lead role in global efforts of commercial satellite operators to foster an interference-free space environment. Intelsat is working with satellite operators, industry groups, customers and equipment manufacturers to make RFI reduction a top priority.

There are both long- and short-term causes of interference.[11] Long-term interference typically occurs between two adjacent satellites and can be caused by lack of coordination between users, outdated or poorly designed equipment, or small mobile antennas. Terrestrial sources, such as microwave links or radar signals may also cause long-term satellite interference. Although it has been rare, interference can also be the result of deliberate, politically motivated actions, such as the recently-reported Iranian jamming of certain western broadcasts. Short-term interference typically results from poor training and operator error. Over 80% of interference events experienced each year result from some form of user error. Proper training is critical for reducing RFI incidents. A majority of RFI incidents are attributed to faulty installation practices, uplink errors and poor equipment maintenance regimes. Intelsat and other leading operators are endorsing new, comprehensive training and certification programs to educate technicians on proper equipment installation and operational parameters.

One concept recently embraced by the global satellite industry is the deployment of "Carrier ID" technology to help identify the interference source. Carrier ID is a stamp on uplink signals that enables satellite operators to more efficiently trace the source of transmissions to their satellites and thereby speed the remediation of any signal interference. Carrier ID would be on every carrier transmitted to the satellite. It is a small identification that may include the operator name, the contact's telephone number, or the modem serial number. The goal is that, at any given monitoring location, a single system can extract the Carrier ID for any and all carrier types

[11] *Carrier ID Using MetaCarrier®* Technology, ComTech white paper, http://www.comtechefdata.com/

where Carrier ID insertion has been provided. This will allow satellite operators to communicate directly with the RFI source to resolve the incident.

The 2012 Summer Olympics in London were the most-watched television event in U.S. history, attracting over 219 million viewers over 17 days of coverage. The London Games were also a perfect opportunity to test Carrier ID technology. The major satellite providers all deployed Carrier ID with positive results.

In addition, the Olympic experiment served as a test bed for a Carrier ID Database. This database was developed in partnership with SDA as an adjunct to the existing work of the organization. The open exchange of operational data is imperative for critical satellite operator procedures, including RFI identification, analysis and RFI geolocation. The Carrier ID Database was designed to be complementary to the other services of the SDA. When implemented, the SDA could then provide a central repository where satellite operators can standardize, formalize and automate data collection.

Although the commercial satellite operators have devoted a considerable amount of time and resources to the issue of RFI and although this issue is of high importance to the U.S. government, there has been very little real coordination on this topic or the larger spectrum topics that face all satellite users. Both DoD and industry are under pressure in the U.S. and around the world to release valuable spectrum, or to share spectrum, with the fast-growing terrestrial wireless industry. As stated above, DoD relies on the commercial sector for the vast majority of its satellite communications requirements, including virtually all of its beyond-line-of-sight UAV communications. The commercial satellite operators have made a number of proposals for more creative sharing regimes, such as hosted payloads and DoD spectrum-

specific commercially operated satellites. To date, DoD has been reluctant to embrace any of these forward-leaning proposals.

Solar Weather Effects on Satellites

The sun is the dominant element in the determination of "space weather" and satellite operators monitor the sun's activities in order to improve their ability to respond to the impact of solar events.[12] There is, occasionally, speculation that the partial or complete disabling of a communications satellite might have been the result of a solar effect. Such reports are the result of analysis and speculation since physical analysis of the satellite is impossible. For the most part, satellite manufacturers build their products to operate in the sometimes-harsh environment of space and satellite operators have come to assume that their satellites will withstand such "weather" events. The goal of satellite fleet operators has been to identify and effectively counter the sun's link to so-called single-event upsets (SEUs), which happen whenever the performance of one or more spacecraft components abruptly changes without warning.

Solar researchers, space weather forecasters and satellite operators focus on four elements of solar weather that can affect satellite communications: solar wind, coronal holes, coronal mass ejections (CMEs) and solar flares. The solar wind is constant but varies in intensity, while the other three solar phenomena are more highly variable. SEUs are not apt to be caused by the solar wind itself, which is relatively low in energy and seldom penetrates the outer layers or protective skin of a spacecraft. Instead, coronal holes, CMEs and solar flares can be more potentially disruptive. When solar storms erupt, they can bombard a satellite with highly-charged particles and increase the amount of charging on the spacecraft's surfaces.

[12] Intelsat. (2013). Solar Weather [White Paper]. Retrieved from www.intelsat.com/tools-resources/satellite-basics/solar-weather/

Coping with electrostatic discharges from the sun that can potentially disrupt satellite services are part of the everyday reality of the satellite world. Losing solar power is not a serious concern whereas losing total control and command of a satellite as the result of solar weather is the most severe effect. Solar panels on satellites are the most affected components, and normal erosion rates for solar panels are usually 0.3% to 1% per year. A solar storm can reduce solar panel performance by 3% to 5% in a day, but since this phenomenon is well understood, spacecraft manufacturers increase the tolerances by design, and attach larger than needed solar panels to a satellite in order to allow for losses during the anticipated solar storms.

The body of a communications satellite, which contains vital control and communication components, is built with special materials as well as active and passive measures so as to be highly resilient to the sun's effect. A so-called "Faraday Cage" protects the satellite's internal equipment from external electrical charges. High-energy particles discharged by the sun rapidly lose strength as they pass through the multiple layers of a spacecraft's body or bus as well. There, they encounter a series of specially designed circuit dividers, individual compartments, and other unique structural elements that act as protection barriers.

The disruptive nature of solar weather impacts far more than satellite operations, and adversely affects terrestrial power and communications grids. For these and other reasons, a considerable amount of manpower and money has been devoted to monitoring the sun's activity, and more research into solar phenomena in general is planned in the future. Among other things, one benefit has been a steady improvement in our ability to rapidly detect and track these solar events using powerful observation and detection systems both on the ground and in space.

NASA, the U.S. National Oceanic and Atmospheric Administration (NOAA) and the DoD oversee much of this activity. For example, besides NASA's twin Solar Terrestrial Relations

Observatory (STEREO) spacecraft, the Air Force Research Laboratory launched the Communication/Navigation Outage Forecasting System (C/NOFS) satellite several years ago to forecast the presence of ionospheric irregularities caused by the sun that adversely impact communication and navigation systems. Ground-based measurements also assist in space weather monitoring.

Satellites depend upon the sun, and satellite operators have steadily developed tools and techniques that allow them to ensure the operational integrity of all satellites in the face of all forms of solar weather. Thanks to proper planning, design and execution, solar events have had, to date, little impact on commercial satellite operations.

Conclusion

Dependable and ubiquitous satellite communication services are critical both to the global economy and to the national security of the United States. Because of the large capital investments required to design, build, launch and operate satellites, commercial operators have a vested interest in doing all they can to protect their spacecraft in orbit from the real threats posed by other objects in space, signal interference, solar weather, cyber-attack and intentional jamming. The U.S. Government also has billions of dollars invested in communications satellites and shares the industry's desire to protect its critical satellite communications capability. Because the Government relies so heavily on commercial satellite capacity, a spirit of cooperation is required to maintain the overall safety of the global satellite fleet, both commercial and Government owned.

Determining the orbit of objects near GEO is a complex task, particularly for uncooperative objects. As the population of objects in the GEO neighborhood grows, maintaining a secure

and highly accurate catalog of all objects becomes increasingly important to mitigate risk of collision and for security of high value assets. The current Space Surveillance Network (SSN) capabilities for tracking these objects are subject to a number of constraints – particularly weather, scheduling, geographic diversity dispersion and overall capacity – which leave the current GEO catalog in significant need of improvement. Recent efforts, within SDA, to share owner-operator data provide clear proof of the value of collaboration.

The Space Data Association was established to allow all satellite operators to cooperate in tracking known objects in space. While NASA and NOAA have both joined in providing information to the SDA database, other U.S. Government agencies – most particularly, the U.S. Department of Defense – have not yet chosen to participate.

In its next evolution, the SDA will employ the resources and relationships it has developed to address the growing issue of radio frequency interference. While the user error that causes most RFI incidents will never be completely prevented, commercial operators now are deploying Carrier ID and developing other tools in place to quickly solve interference problems. However, this only applies to commercial satellites. Currently, there is little coordination between Government and industry when government-owned satellites are involved. This is an area where better cooperation could ensure that space assets are available to all users when they are needed.

In creating the SDA, the private sector has taken the first step towards a new paradigm for managing risk in space, but to be most effective, far more cooperation is needed by both commercial and government satellite operators worldwide.