THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Commercial Satellite Communications Mission Assurance

November 2009

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Over the last decade, the Federal Government has become increasingly reliant on the commercial satellite communications industry. Today, the satellite industry is providing voice, data, and video services in support of Government operations, including national security and emergency preparedness (NS/EP) missions. The commercial industry is also supplying the majority of the satellite communications used for military operations in Afghanistan and Iraq. As part of the Nation's critical infrastructure, satellite networks provide unparalleled coverage of remote geographical areas and difficult terrain. They complement terrestrial networks also used to provide NS/EP communications support.

In response to a request from the National Security Space Office (NSSO), the President's National Security Telecommunications Advisory Committee (NSTAC) reestablished a Satellite Task Force in November 2008 to review the March 2004 NSTAC *Satellite Task Force Report* (*2004 Report*), including its Vulnerabilities Triage. The NSSO asked the 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.

The NSTAC sought information from NSTAC member companies, subject matter experts (SME) from non-NSTAC commercial satellite companies, and relevant Government stakeholders. Specifically, the NSTAC: (1) examined the *2004 Report* to identify new developments within the commercial industry; (2) reviewed the *2004 Report* recommendations and implementation status; (3) updated the Vulnerabilities Triage to reflect the current environment; (4) engaged satellite industry SMEs and Government stakeholders to provide briefings on a broad spectrum of subjects relevant in today's commercial satellite environment; and (5) conducted two industry questionnaires via the Satellite Industry Association regarding physical and cybersecurity to validate the report's findings and provide additional insight to the SME briefings and stakeholder inputs.

The NSTAC developed conclusions in the following nine areas: (1) radio frequency interference (RFI); (2) cybersecurity; (3) avoiding collisions in space; (4) measures and investments for terrestrial infrastructure; (5) command encryption on commercial satellites; (6) Mission Assurance Working Group; (7) long-term requirement planning challenges; (8) commercial satellite industry innovation; and (9) space weapons.

The NSTAC concluded that radio frequency interference represents a significant and growing threat to satellite services, including NS/EP missions. Most instances of interference stem from user error due to lack of adequate user training, equipment failure, or poor operational practices and are very rarely deliberate. Government and industry do not collaborate systematically to share information regarding the detection, characterization, geolocation, and mitigation of interference. Today, the Government engages with industry only when a Government service is affected instead of working collaboratively with industry to identity best practices and establish shared situational awareness and mitigation approaches.

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.

Satellites are far less likely than terrestrial facilities to be the target of a successful physical attack due to their location in space. While an accidental collision between space debris and a satellite is unlikely, collisions do occur, can be catastrophic, and cause permanent damage. The February 2009 collision of an Iridium communications satellite and a defunct 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 the DoD's Commercial and Foreign Entities Program and industry's Space Data Association should promote better location sharing, maneuver coordination, and collision avoidance.

The NSTAC found that satellite operators use redundant and geographically diverse facilities to protect terrestrial infrastructure from man-made and natural threats and 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.

Consistent with Government policy, most satellite companies use the National Security Agency-approved satellite command uplink encryption for satellites supporting U.S. Government services. As operators replace their older, legacy satellites that are technically incapable of encrypting commands, newer satellites are likely to be fully compliant with the Government's policy direction.

Since its inception in 2006, and as a result of the *2004 Report*, the Mission Assurance Working Group (MAWG) has built a constructive and collaborative relationship between DoD and the satellite industry. The MAWG has 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. The MAWG also exchanges sensitive U.S. Government security-related information with cleared industry personnel whose systems support national security and military forces.

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.

Commercial satellite systems are being enhanced with increased capacity and quality of service to better support commercial and Government needs, including NS/EP. Recent developments in next generation satellite technology include systems with multiple spectrally efficient spot beams that may mitigate the effects of purposeful interference and satellites with onboard packet processing, facilitating full mesh networks and reducing end user reliance on centralized Earth stations. Additional innovations include the implementation of enhanced cybersecurity measures by leveraging terrestrial network technologies. While commercial satellite providers have demonstrated the functionality and utility of packet processing satellites, future studies are needed to completely identify new threats specific to next generation satellite systems.

Finally, the NSTAC concluded that due to the technological availability and/or cost of mitigation, the commercial satellite industry does not mitigate the risk of certain space threats such as nuclear detonations or space weapons, or ground communications and control segment threats from chemical, biological, and radiological agents.

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:

- **Direct the Secretary of Homeland Security to establish, consistent with the conclusion of the NSTAC *Cybersecurity Collaboration Report,* an operational mechanism for the Government and private sector to collaborate and coordinate to prevent, detect, mitigate, and respond, in a trusted environment, to cyber threats and cyber events**.
  - –Establish a Government-sponsored Joint Coordinating Center (JCC) for satellite industry representatives and other critical infrastructure and key resources sector stakeholders. The JCC's primary mission would focus on robust information sharing to develop and share cyber situational awareness, and would institutionalize the time-sensitive processes and procedures to detect, prevent, mitigate, and respond to cyber incidents of national and international consequence.
  - –The JCC would build upon the current capabilities of the National Coordinating Center for Telecommunications and the U.S. Computer Emergency Readiness Team, and incorporate other existing cyber incident monitoring and response entities.
  - –The JCC capability should be located in a Government facility with continuous operations, supporting tools, and collaboration capabilities.

- **Direct the Secretary of Defense and Secretary of Homeland Security to fund a comprehensive information sharing and operational collaboration program with key industry partners to systematically reduce electromagnetic interference (EMI) and RFI**.
  - –The Government should establish a single joint industry-Government collaboration center to address planning and operational EMI/RFI issues.

- –Early efforts between the DoD's Global Satellite Communications (SATCOM) Support Center (GSSC) and industry, though focused on DoD, indicate that better integration between Government and industry on planning and operational matters would yield substantial benefits and help mitigate significant EMI/RFI vulnerabilities; the GSSC is one candidate to become the single Government focal point.
- –DoD continues to develop and field systems to detect, identify, geolocate, and report on satellite service interference from both unintentional and deliberate sources. The level of proposed operational interaction and information sharing between DoD systems and the commercial satellite industry remains unclear, but such systems could become useful tools to help support commercial operator efforts to address interference.

- **Direct the Secretary of Defense to make safety of flight and the preservation of the space environment the leading national security drivers for enhanced space situational awareness efforts**.
  - –The U.S. Government has a strong interest in preserving the space environment. Through improved data collection and processing, and close collaboration with industry, the Government can play an important role in encouraging safe and responsible space flight operations and can avoid the creation of unnecessary, dangerous space debris. In particular, DoD should:
    - o Continue and expand the Commercial and Foreign Entities Program under which the U.S. Government currently shares orbital information with the private sector. In particular, the Secretary of Defense should provide high-accuracy Government data on existing space debris to all space operators and routinely share operational and flight data with commercial service providers. The data exchange between the U.S. Government and commercial operators should be automated to the greatest extent possible, and should include the most accurate, operator-supplied data on satellite locations and planned maneuvers. DoD, in conjunction with commercial operators, should begin to develop common operational protocols for handling routine and emergency situations.
    - o Augment existing space surveillance capabilities through innovative programs such as hosting Government payloads/sensors on commercial satellites. Every satellite launched into space is potentially a sensor that can help extend the capabilities of an evolved Space Surveillance Network.
    - o In conjunction with the Secretary of State, begin an international dialogue with other nations on space data sharing with the goal of merging national space catalogs and sensor data to create a more complete view of the space environment.

- **Direct the Secretary of Defense and the Secretary of Homeland Security to plan, in consultation with industry, for future satellite services, and to establish and enforce a uniform set of U.S. Government-wide mission assurance requirements (similar to that of the current DoD Defense Information Systems Network [DISN] Satellite Transmission**

Services-Global [DSTS-G] model) for fixed and mobile satellite communication providers serving the NS/EP community.

- –Satellite operators routinely plan to replace existing satellites with updated or enhanced systems to meet commercial and potential Government user requirements. Unlike other commercial satellite users, the Government does not engage with industry in planning its long-term communication needs. Typically, funding for DoD commercial SATCOM mobile and fixed satellite services comes from one-year increments of supplemental funding, as opposed to programmed funding lines, making long-term forecasting difficult. As a result, the Government relies entirely on the "spot market" to meet long-term service needs, risking shortfalls in commercial satellite availability when critical needs arise. Representatives from the Government should meet with the commercial satellite industry no less than annually to engage in planning long-term communications needs.
- –Some satellite operators have made substantial investments in new systems and procedures to meet evolving mission assurance requirements. The Government should build on the experience it has gained in the implementation of the information assurance process in the current DSTS-G contract to uniformly enforce its information security requirements for all of the satellite contracts that it awards. New processes should be implemented in a manner that provides an incentive for commercial providers to maintain and upgrade the security and integrity of networks used for critical NS/EP functions.
- –The Government should make appropriate investments to ensure the availability of satellite-based priority communication services necessary to increase the robustness and reach of NS/EP Government communications, both before and during an emergency.
- –Fund research and development to evolve key satellite solutions such as multiple spot beams and unified packet processing systems to enable next generation networks for integrated voice, video, and data services.

1.0 INTRODUCTION

In recent years, the commercial satellite communications (COMSATCOM) industry has significantly increased its support to Government users, supplying a wide range of advanced voice, data, and video communications services. The uniquely flexible nature of satellite networks offers mobile communications services, ubiquitous coverage over large geographic areas, and greater access to remote areas or difficult terrain. Satellite networks can quickly provide surge capacity to aide in terrestrial critical infrastructure restoration efforts in the event of an emergency or crisis operation. Meanwhile, U.S. reliance on satellites for military and economic success has grown dramatically in recent years, making protection of space assets a priority. As a result, the need to protect space assets has increased.[1] Currently, commercial satellite systems provide over 85 percent of the Department of Defense's (DoD) global satellite communications (SATCOM), and commercial satellite links are used to operate almost all unmanned aerial vehicles in Afghanistan and Iraq. The DoD also estimated that 80 percent of the satellite communications capacity used for Operation Iraqi Freedom was provided by commercial satellites.[2] Figure 1 below depicts the DoD's increasing expenditures and use of commercial fixed satellite service bandwidth.

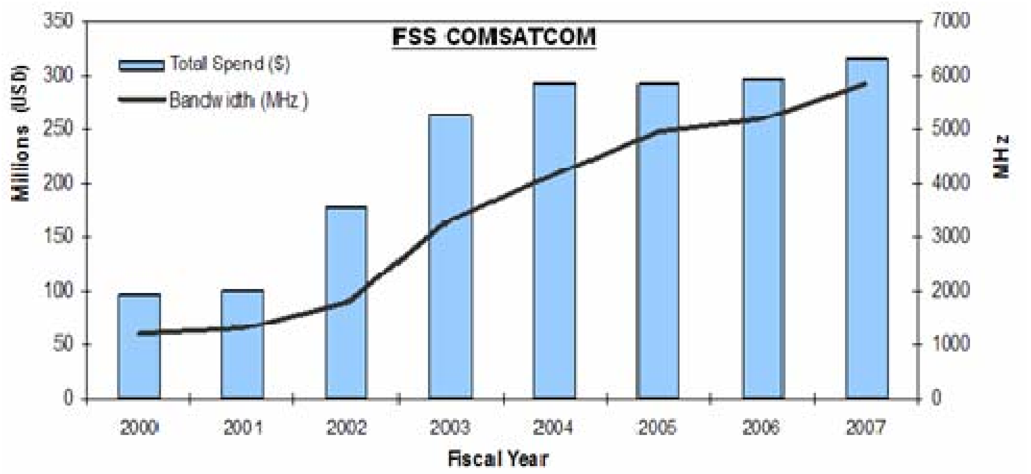

Figure 1 Department of Defense Fixed Service Satellite Expenditures vs. Bandwidth Over Time[3]

Services offered by the commercial satellite industry are critical to maintaining national security and emergency preparedness (NS/EP) communications and mission assurance because satellites: (1) offer primary and back-up communications; (2) facilitate continuity of operations services; (3) offer customers point-to-multipoint communications; (4) serve as an alternative in the event of a terrestrial wireline or wireless network outage; (5) provide restoration services to terrestrial critical telecommunications and utilities (oil, gas, electricity, and water) infrastructure; (6) offer

[1] Burke, Alan W. "Space Threat Warning: Foundation for Space Superiority, Avoiding A Space Pearl Harbor," Air War College Research Report 2006.

[2] Williamson, M. "Encryption and Satellite Security," Transmission Security, p. 38-41, March/April 2006.

[3] Source: U.S. Strategic Command, *FY07 Commercial Satellite Communications (COMSATCOM) Usage Report (FOUO)*, February 6, 2009.

diversified and distributed commercial owner/operator facilities; and (7) reside in an environment that makes assets highly resistant to many natural and terrestrial effects.

Satellite communications are a part of the Nation's critical infrastructure, identified as such various Executive Orders[4] and Presidential Directives,[5] that provide key communications capabilities to the Federal Government. See Appendix H for high-level descriptions of the Executive Orders and Presidential Directives that support the requirement to use satellite communications during emergencies and for continuity of Government.

1.1 Charge

The National Security Telecommunications Advisory Committee (NSTAC) Industry Executive Subcommittee reestablished the Satellite Task Force (STF) during its November 2008 Working Session at the request of the National Security Space Office (NSSO). The NSSO asked the NSTAC to review the 2004 *Satellite Task Force Report* and evaluate the following questions:[6]

- What are the top cyber infrastructure threats facing the commercial satellite industry?
- What countermeasures and operating tools are in place to address these threats?
- How does the Government's use of integrated networks, public and satellite, to transmit sensitive data affect its cybersecurity[7] strategy?
- How might attempts to develop a standard security framework among satellite operators serve to enhance national security?
- How are satellite ground stations; teleports; network operation centers (NOC); satellite operations centers (SOC); and telemetry, tracking and command (TT&C) sites protected against physical attack?
- How are NOC, SOC, and TT&C sites protected against biological, chemical, and radiological attacks?
- How are satellite facilities designed to withstand local environment extremes, such as hurricanes, seismic events, and blizzards?

[4] *Executive Order 12472 - Assignment of National Security and Emergency Preparedness Telecommunications Functions*, April 23, 1984; *Executive Order 13407 - Public Alert and Warning System*, June 26, 2006.

[5] *Presidential Decision Directive/NSC-63 Critical Infrastructure Protection*, May 22, 1998; *Homeland Security Presidential Directive / HSPD-7 - Subject: Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003; *Homeland Security Presidential Directive / HSPD-8 - Subject: National Preparedness*, December 17, 2003; *National Security and Homeland Security Presidential Directive / NSPD 51 / Homeland Security Presidential Directive / HSPD 20*; May 9, 2007.

[6] This report focuses primarily on commercial satellite systems. However, many military systems share some or all of these vulnerabilities. DoD operates highly protected systems such as MILSTAR and Advanced Extremely High Frequency, which have anti-jam capabilities and are nuclear-hardened. However, the majority of military satellite systems such as Defense Satellite Communications System, Ultra High Frequency, Wideband Global SATCOM, and the future Mobile User Objective System are not considered "protected" communications systems.

[7] No formal, accepted definition of cybersecurity currently exists. However, the International Telecommunication Union recently approved ITU-T X.1205 "Overview of Cybersecurity." In this document, cybersecurity is defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."

The NSSO also requested that the NSTAC recommend mitigation policies that would maintain the highest level of mission assurance on COMSATCOM networks, and that the NSTAC review the Vulnerabilities Triage contained in the 2004 *Satellite Task Force Report* to reflect commercial industry's concerns and the issues relevant to today's satellite infrastructure. While many issues raised in the 2004 *Satellite Task Force Report* should be examined in future studies, this report addressed only the security aspects requested by the NSSO due to time and resource constraints.

1.2 Approach

In conducting a review of the 2004 *Satellite Task Force Report*, associated recommendations, and the Vulnerabilities Triage, the NSTAC identified and engaged subject matter experts (SME) in the fields of satellite infrastructure, satellite security, and cybersecurity. SMEs briefed the task force on a wide variety of issues including common threats to satellite infrastructure, mitigation and countermeasures, and future trends. Task force members included representatives from NSTAC member companies, SMEs from non-NSTAC commercial communications companies, and Government participants.[8]

To gain a broader understanding of the physical and cybersecurity concerns of terrestrially based communications counterparts, the NSTAC reviewed the November 2008 *NSTAC Report to the President on Physical Assurance of the Core Network (FOUO)*, which discussed physical threats to communications networks from natural or environmental sources,[9] intentional or targeted acts, and unintentional and accidental occurrences. During the NSTAC's Core Assurance study,[10] the satellite working group developed a questionnaire that was distributed to Satellite Industry Association (SIA) members. The questionnaire asked respondents to identify physical threats to satellite systems and mitigation measures in place to protect personnel and physical infrastructure such as buildings and assets. The NSTAC used the data collected by this questionnaire to document the commercial sector's current physical security concerns and mitigation measures in place to combat threats.[11]

To address emerging cybersecurity issues, the task force examined the White House *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* and the May 2009 NSTAC *Cybersecurity Collaboration Report* to gain working definitions and identify the concerns related to the cyber environment. These reports provided a basis for discussion and a common language through which the NSTAC examined the threats and vulnerabilities unique to the satellite industry.[12] To augment these reports, SIA distributed

[8] See Appendix A for a comprehensive list of participants and contributors.

[9] As described in the 2007 Strategic Homeland Infrastructure Risk Assessment threats and the Federal Emergency Management Agency's National Planning Scenarios.

[10] While the initial focus of the Core Assurance effort included satellite-based facilities, the Government requested that the NSTAC remove all satellite-specific material from the report to undertake the 2009 *NSTAC Report to the President on Commercial Satellite Communications Mission Assurance*.

[11] See Appendix C for a copy of the physical security questionnaire and Appendix D containing the high-level results of the physical security questionnaire.

[12] The *Cyberspace Policy Review* cites *National Security Presidential Directive 54 / Homeland Security Presidential Directive 23* (NSPD-54/HSPD-23), which defines cyberspace as, "the independent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and

another questionnaire on behalf of the NSTAC that focused on identifying cybersecurity threats and mitigation measures.[13]

The NSTAC found that cyber and physical vulnerabilities of the terrestrial components of large satellite networks differ in only minor degrees from the networks of traditional terrestrial service providers; therefore, this report will not focus on common topics and vulnerabilities that have been covered at length in other NSTAC reports.[14] The 2009 *NSTAC Report to the President on Commercial Satellite Communications Mission Assurance* instead focuses on the cyber and physical vulnerabilities specifically related to SATCOM systems.[15]

Finally, the task force revised the Vulnerabilities Triage contained in the 2004 *Satellite Task Force Report*. The Triage identified the threats to elements of satellite infrastructure, vulnerability to each threat, the impact of an attack on satellite infrastructure, and potential techniques used to mitigate vulnerabilities. The Vulnerabilities Triage includes rankings on a 1-5 scale that detail the relative costs required to carry out or mitigate the potential threat and the projected level of impact if the threat occurs. In its review, the NSTAC reorganized the existing matrix and changed the top-level categories to consolidate and align the information, examined the cost structure to determine where changes were required, and added new threats relevant to today's threat environment. For more information on the Vulnerabilities Triage, please contact the National Communications System (NCS) at nstac1@dhs.gov.

1.3 Commercial Satellite Industry Overview

The commercial satellite industry provides global services to a wide range of commercial and Government users; key market segments include media, network services, and Government services. From 2003 to 2008, satellite industry revenues worldwide increased an average of 14.2 percent year-over-year. From 2007 to 2008, revenue generated from satellite communications and services, manufacturing, launches, and equipment increased 19 percent to $144.4 billion.[16]

embedded processors and controllers in critical industries. Common usage of the terms also refers to the virtual environment of information and interactions between people."

[13] See Appendix E for a copy of the cybersecurity questionnaire; Appendix F contains the high-level results of the cybersecurity questionnaire.

[14] NSTAC *Cybersecurity Collaboration Report*, May 2008; *NSTAC Report to the President on Physical Assurance of the Core Network (FOUO)*, November 2008; *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic*, November 2008; *NSTAC Report to the President on Network Operations Centers (FOUO)*, February 2008; *NSTAC Next Generation Networks Task Force Report*, March 2006; NSTAC *Federal Support to Telecommunications Infrastructure Providers in National Emergencies*, January 2006; *Next Generation Networks Task Force: Near Term Recommendations Working Group Report*, March 2005; *NSTAC Trusted Access Task Force Report on Screening, Credentialing, and Perimeter Access Controls*, January 2005; *NSTAC Vulnerabilities Task Force Report on Concentration of Assets: Telecom Hotels*, February 2003; *NSTAC Vulnerabilities Task Force Report on Trusted Access to Telecommunications Facilities*, March 2003; *NSTAC Vulnerabilities Task Force Report on Internet Peering Security*, March 2003.

[15] The House Armed Services on July 10, 2008, heard the testimony of Chairman Graham on the threat posed by Electromagnetic Pulse (EMP) attack. http://armedservices.house.gov/calendar_past_hearings.shtml.

[16] Satellite Industry Association, *State of the Satellite Industry Report*, June 2009.

Today's large, global satellite operators are often multinational organizations that maintain complex hybrid networks composed of both terrestrial and space assets. The satellite component of a hybrid communications system consists of a number of subcomponents:

- The satellite bus maintains the satellite's position in orbit, produces power, manages thermal loading, maintains payload configuration management, and facilitates telemetry and orbital control operations;
- The communications payload and its related antennas allow the satellite to be used as a communications node;
- The ground control segment (the SOC) "flies" the satellite and manages the associated TT&C sites necessary to command the satellite;
- The ground communications segment (the NOC) controls the payload onboard the satellite, monitors network operations, and assists in solving connectivity and network problems;
- Earth stations communicate through satellites, typically with small antennas and low-cost electronics at user facilities, and large antennas with more complex data handling facilities at key traffic hubs; and
- Satellite uplinks and downlinks transmit information between the satellite and the operations center, other facilities, or users.

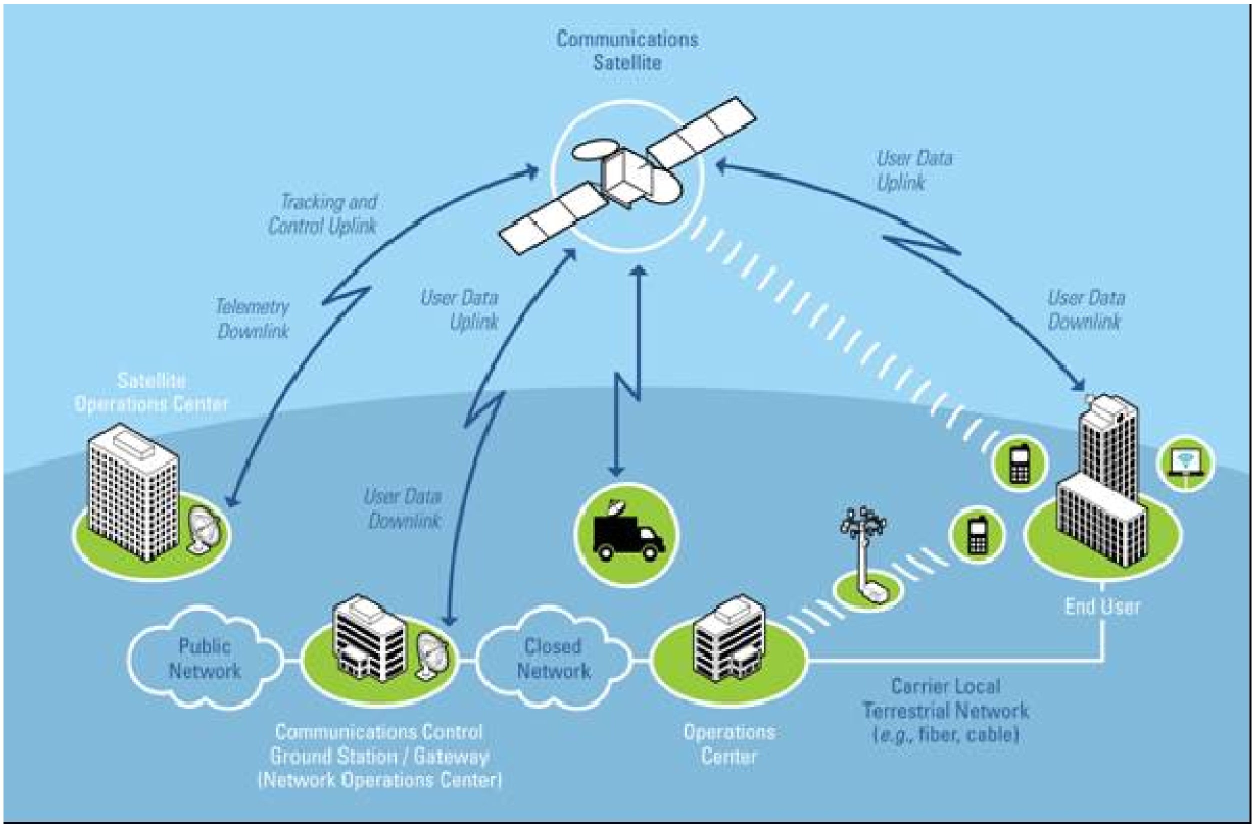
Communications Satellite
Tracking and Control Uplink
Telemetry Downlink
User Data Uplink
User Data Uplink
User Data Downlink
User Data Downlink
Satellite Operations Center
Public Network
Closed Network
Communications Control Ground Station / Gateway (Network Operations Center)
Operations Center
Carrier Local Terrestrial Network (e.g., fiber, cable)
End User

Figure 2 Hybrid Satellite / Terrestrial Communications Networks

Figure 2 represents how typical satellite systems are integrated into terrestrial-based segments of modern converged networks, including all satellite-specific components identified above, with links to ground stations, the public Internet, local end users, and communications on the move.

1.4 Results of the 2004 Satellite Task Force Report

In January 2003, the President's NSTAC established the STF at the request of the Director, National Security Space Architect, to conduct a study of COMSATCOM systems infrastructure protection mechanisms. The NSTAC: (1) reviewed applicable documentation addressing vulnerabilities in the commercial satellite infrastructure; (2) identified potential policy changes that would bring the infrastructure into conformance with a standard for mitigating those vulnerabilities; (3) considered Global Positioning System timing capabilities during the deliberations;[17] (4) coordinated its response with representatives from the NCS, 14 Federal departments and agencies, and SIA members; and (5) in March 2004, published the *Satellite Task Force Report*, which included findings and Presidential-level recommendations.

The 2004 report documented the benefits of commercial satellite use in NS/EP missions and suggested that if correctly employed, satellites could function as a reliable back-up to the public switched telephone network (PSTN), increase communications resiliency and system redundancy, and provide transmission media diversity. Satellite networks have the ability to bypass, or interconnect with, terrestrial networks in the event that those networks become unavailable or congested, allowing operators to re-route traffic and thereby increase overall end-to-end communication availability.

The 2004 report concluded that certain components of COMSATCOM systems, such as terrestrial satellite ground and control segments, were more susceptible to sophisticated physical attacks than the space segment. While commercial operators that did not employ encryption in satellite command links were at an increased risk, many carriers implemented the physical infrastructure security and cybersecurity measures deemed necessary to protect commercial business. At the time the 2004 report was drafted, the satellite industry and the Federal Government maintained no clear lines of communications, responsibility, or coordination mechanisms to conduct long-term planning and ensure that the Government could effectively meet its responsibilities in the event of an emergency. Finally, the study revealed that many agencies lacked the in-house expertise to properly integrate COMSATCOM services into their communications architectures and that Government procurement processes hindered its ability to efficiently compete for COMSATCOM capacity.[18]

The 2004 NSTAC *Satellite Task Force Report* recommended that the President:

- Direct the Assistant to the President for National Security Affairs, Assistant to the President for Homeland Security, and Director, Office of Science Technology Policy, to develop a national policy with respect to the provisioning and management of commercial SATCOM services integral to NS/EP communications, recognizing the vital and unique capabilities

[17] *NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS)*, February 2008.
[18] NSTAC *Satellite Task Force Report*, March 2004.

commercial satellites provide for global military operations, diplomatic missions, and homeland security contingency support.

- Fund the Department of Homeland Security to implement a commercial SATCOM NS/EP improvement program within the NCS to procure and manage the non-Department of Defense satellite facilities and services necessary to increase the robustness of Government communications.
- Appoint several members to represent service providers and associations from all sectors of the commercial satellite industry to the NSTAC to increase satellite industry involvement in NS/EP.

1.4.1 Government and Industry Response to 2004 Recommendations

The 2009 effort reviewed each recommendation contained in the 2004 report and concluded:

- Since the publication of that report, the DoD Executive Agent for Space, Commander of U.S. Strategic Command (USSTRATCOM), and the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) have worked in conjunction with the COMSATCOM industry to address issues of mutual concern. The DoD established the Mission Assurance Working Group (MAWG), which is composed of satellite SMEs from the COMSATCOM industry and representatives from relevant Government departments and agencies.
- The Department of Homeland Security (DHS) did not implement a COMSATCOM NS/EP improvement program. Only DoD took steps to develop a program to improve the Government's use of COMSATCOM, and those efforts were strictly limited to DoD.
- The President appointed a satellite provider as a member of the President's NSTAC.

Mission Assurance Working Group

In response to the first recommendation, the DoD Executive Agent for Space established the MAWG on May 10, 2006, as a standing forum under the DoD's NSSO with a focus on enhancing SATCOM services and mission assurance related to U.S. national security interests, and addressing threats that affect the United States and its allies. Under the leadership of the NSSO in conjunction with USSTRATCOM, ASD/NII, and Defense Information Systems Agency (DISA), the MAWG engages the DoD and COMSATCOM companies to explore policy, planning, architecture, programs, and processes in support of U.S. national security interests. The establishment of the MAWG was also critical in helping a small number of key individuals from multiple commercial owner/operator organizations obtain SECRET level security clearances, without which industry experts could not participate in classified meetings with Government stakeholders to discuss threats and vulnerabilities to the space sector. Prior to this time, very few private sector companies employed individuals who possessed a DoD clearance. As part of the MAWG process, Government entities such as the National Air and Space Intelligence Center provide periodic intelligence briefings to share insight into potential threats to satellite operations posed by malicious actors.

Commercial Satellite Communications NS/EP Improvement Program

Through the second recommendation, the NSTAC suggested that DHS, with the assistance of the NCS, procure and manage non-DoD satellites and services for NS/EP and that each agency examine its own network to determine if it adequately utilized satellites for more robust networks, identify whether satellite data came through single points of access, or diversify routing. This activity was never completed.

Appointment of Satellite Providers to the NSTAC

In response to the third recommendation, the President appointed PanAmSat Corporation[19] to the President's NSTAC to represent the commercial satellite industry in discussions related to NS/EP communications. Today, the NSTAC reaches out to commercial satellite companies and other industry organizations to identify and leverage satellite expertise not resident within the NSTAC.

1.5 Government and Industry Developments on Cyber Threat Reduction

In response to increased satellite network usage for Government-related functions and to further protect Government traffic running over commercial satellite networks, the Government has adopted guidelines to try to ensure that the satellite capacity it purchases meets certain minimum levels of security and availability.

1.5.1 Mission Assurance Requirements

According to participants in this effort, DoD purchases the most commercial satellite bandwidth of U.S. Government users, the majority of which is purchased by DISA through a contract vehicle known as the Defense Information Systems Network (DISN) Satellite Transmission Services-Global (DSTS-G) contract for Fixed Satellite Services. In May 2007 DISA amended the DSTS-G contract to comply with National Security Telecommunications and Information Systems Security Policy[20] used by the DoD. The DSTS-G modification established a number of mission assurance requirements, including: (1) employing TT&C command link encryption; (2) facility and personnel security clearances; (3) electromagnetic interference (EMI)/ radio frequency interference (RFI) geolocation capabilities; (4) communications security (COMSEC) access through secure voice and data facilities; and (5) other information assurance and protection requirements for information systems. These requirements obligate each commercial satellite service operator seeking to supply bandwidth services to DSTS-G to submit compliance documentation with each bid.[21]

DISA categorizes its satellite communications task orders into three Mission Assurance Category (MAC) levels, based on DoD Instruction (DoDI) 8500.2 and National Institute of Standards and Technology Special Publication (NIST SP) 800-53, in order to assist in determining availability and integrity requirements[22] and to demonstrate the advantages of more secure ground stations and traffic flow through satellites with encrypted TT&C. MAC I designates information deemed to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. MAC II designates information that is important to the support of deployed and contingency forces. MAC III designates information that is

[19] Intelsat completed its acquisition of PanAmSat in 2006; Intelsat is now a member of the President's NSTAC.

[20] National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 12, Subject: *National Information Assurance (IA) Policy for U.S. Space Systems and Directive 8581.1, Information Assurance (IA) Policy for Space Systems*.

[21] Department of Defense Instruction 8500.2, Information Assurance (IA) Implementation, February 2003. In March 2007, NSTISSP 12 was superseded by Committee on National Security Systems Policy No. 12, Subject: *National Information Assurance Policy for Space Systems Used to Support National Security Missions*.

[22] Department of Defense Instruction 8500.2, Information Assurance (IA) Implementation, February 2003.

necessary for the conduct of day-to-day business but does not materially affect support to deployed or contingency forces in the short-term. Further, each satellite communications task order is categorized by confidentiality level, based on whether the system processes classified, sensitive, or public information—creating nine total combinations.[23]

In April 2008, DISA developed and began the implementation of "the best value methodology" for considering this information in the context of evaluating task orders. Under the best value methodology, proposals that meet or exceed security requirements would be preferred over other technically compliant proposals that contain a greater information assurance (IA)/protection risk posture. This methodology includes certification and accreditation of the proposed solution, documents the risks associated with the proposals, and requires an informed consent agreement with the end user. In the early implementation of this methodology, satellite operators often felt that bearing the costs of additional security did not provide any competitive advantage over less expensive, less compliant solutions.

Since implementation of this best value methodology, DISA has continued to refine and improve the processes and options for operators. Operators may obtain SECRET facility security clearance approval, security clearances for personnel, and access to secure voice and data communications to support incident response. These measures have helped to address initial industry concerns. Today, DSTS-G is the only significant Government COMSATCOM contract mandating compliance with national information assurance and protection requirements.

Other Government entities are also increasing their focus on satellite security for future contract awards. For example, the Navy has been aggressive in its pursuit of IA by requiring bidders on its Commercial Broadband Satellite Program to submit to the full DIACAP Process (Defense Information Assurance Certification and Accreditation Process).[24] The Navy has also recognized the need to compensate suppliers explicitly for implementation of IA and made provisions for a specific contract line item number (CLIN) to be used for this purpose.

As a result of this increased focus on security, commercial satellite providers today are providing end-to-end, defense-in-depth network solutions to Government requirements that take into account risk assessments and provide strong, effective, multi-layer, multi-dimensional protections. During the design phase of a new network, commercial operators develop defense-in-depth technical layers consistent with the customer's overall security criteria and risk assessment, and where needed will identify and acquire the information technology and IA products—commercial off the shelf (COTS) hardware, firmware, software and other products, including products that have been evaluated as compliant with DoD IA standards outlined in DoDI 8500.2.

[23] Ibid.

[24] DIACAP is the process for certification and accreditation of all DoD information systems and for determining whether these systems need be authorized to operate on DoD networks, including the Global Information Grid (GIG). DIACAP contains the DoD processes for identifying, implementing, validating, certifying, and managing information assurance measures and services, expressed as Information Assurance Controls, and authorizing the operation of DoD information systems in accordance with statutory requirements, including the *Federal Information Security Management Act* (FISMA). DIACAP implements information assurance controls based on information assurance MAC and Confidentiality Level. DIACAP is a comprehensive certification and accreditation process that supports and complements the net-centric GIG-based environment.

Operations are a critical element of the reconstitution in the aftermath of an attack. Industry operations teams routinely perform assessments and provide proactive monitoring and control against intrusions, and once identified move aggressively to reconstitute the system to mitigate the intrusion. Employees fully trained in system security administration are critical in providing in-depth defense for end-to-end networks.

1.5.2 Future COMSATCOM Services Acquisition

In August 2009, DISA and the General Services Administration (GSA) announced their "Future COMSATCOM Services Acquisition (FCSA)" acquisition strategy, which will allow all Federal customers to procure commercial satellite bandwidth, subscription services, and customized end-to-end solutions from a common marketplace. FCSA's scope includes current services available on DSTS-G, GSA SATCOM II, and DISA Inmarsat contracts.[25] Reaffirming the requirements found in DSTS-G, the DISA/GSA team noted that future awardees must include cyber protection requirements, including:

- Network operations monitoring and fault reporting consistent with commercial/industry standards and/or best practices; and
- Commercial solutions addressing Federal IA and protection requirements:
  - *Federal Information Security Management Act*, December 2002.
  - Committee on National Security Systems Policy (CNSSP) No. 12, Subject: *National Information Assurance Policy for Space Systems Used to Support National Security Missions*, March 2007.
  - NIST SP 800-53 *Recommended Security Controls for Federal Information Systems and Organization*, August 2009.
  - Department of Defense Directive 8581.1, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*, June 2005.

[25] Further information available at: http://www.gsa.gov/fcsa

2.0 THREATS COMMON TO COMMERCIAL COMMUNICATIONS SERVICES

Modern communications networks are composed of a complex mix of technologies. In some cases, the network's entire transmission path is physical, while in other cases the transmission path includes wireless radio or optical links, such as satellite links or terrestrial mobile services.[26] Conceptually, threats to commercial satellite services can be characterized in the same way as those threats facing other terrestrial and wireless communications technologies.

- **Physical Threats**: Destruction of physical network infrastructure, or physical threats to operational personnel. Examples include explosions, cable cuts, hostage-taking at control centers, natural disasters, power failures, satellite collisions, and space-based attacks.
- **Access and Control Threats**: Unauthorized access, control, or prevention of the operator's control of its network, underlying devices, control links, and physical plants. Examples include unauthorized commanding of or preventing control of routers, switches, servers, databases, or satellite buses used to control the network; distributed denial of service attacks against network control infrastructure; compromise of network security protocols; and actions by malicious insiders.
- **User Segment Threats**: Events, such as denial of service attacks, that occur on user traffic paths of the network that degrade or deny service to users by exhausting or preventing customer access to network resources. Examples include botnets, denial of service attacks, route hijacking, viruses, worms, and RFI.

Satellite-based services are quite similar to terrestrial alternatives with respect to their vulnerability to, and protection from, physical and cyber threats (see Figure 2). Communications satellite networks often contain the same subsystems as their terrestrial counterparts that are vulnerable to malicious and inadvertent disruption—switching, routing, addressing, and authentication nodes. Thus, the mitigation techniques required to secure networks using communications satellites are essentially the same as those required to secure any other network including Internet Protocol (IP); the PSTN; radio networks; and wireline networks such as fiber to the premises, cable, and digital subscriber lines. Much as a fiber can be cut, a wireless satellite transmission can be temporarily interrupted by harmful radio frequencies (RF). Some threats, such as insider threats, cannot be completely mitigated by any communications network operators. However, practices such as personnel background checks, badge display requirements, and appropriate oversight can partially mitigate this vulnerability.

[26] Wireless data services include personal digital assistant devices such as the BlackBerry and iPhone, as well as point-to-point terrestrial microwave links. In many cases end users are unaware of the blend of technologies used to deliver their services.

3.0 VULNERABILITIES AND THREATS OF SPECIAL CONCERN TO SATELLITE SYSTEMS

While satellite systems encounter many of the same threats experienced by terrestrially based counterparts, satellite systems also have unique components that create vulnerabilities requiring additional considerations and mitigation measures.[27]

3.1 Physical Threats

Physical threats to satellite infrastructure span a range of intentional and unintentional actions, and can affect each portion of the network from the assets on the ground to the satellites in space.

3.1.1 The Space Environment—Collisions

Communications satellite operators have achieved a high level of satellite system availability—generally greater than 99.995 percent. Satellites are designed and built with multiple redundant subsystems in place to withstand the natural hazards of the harsh space environment over their multi-year useful lifetime. However, because in most cases satellites cannot be repaired once placed in space, catastrophic physical damage in orbit is usually permanent.[28]

Due to their location in space—a geostationary satellite is 35,786 kilometers (km) from the Earth's surface—satellites and their payloads are less susceptible than terrestrial facilities to physical attack. Military communications satellites hold little advantage over commercial satellites with respect to kinetic threats. Such attacks on a satellite would be exceptionally expensive to conduct, would require unique expertise, and would be difficult for a malicious actor to execute.[29,30]

Sophisticated space powers do have the ability to carry out attacks on space objects. On January 11, 2007, China conducted its first successful test of an anti-satellite (ASAT) missile to purposely destroy the aging Fengyun-1C meteorological satellite that had been in Low Earth Orbit (LEO) since May 10, 1999. The event occurred approximately 850 km above Earth, and created a debris field representing the single worst contamination of LEO in the past 50 years. Within a month the debris cloud expanded in altitude from 200 km to more than 4000 km.[31] Two years later, the U.S. Space Surveillance Network (SSN)—a combination of 29 radar and optical sensors—catalogued a total of 2,378 pieces of debris five centimeters (cm) or greater in diameter resulting from the ASAT test and estimated that 150,000 pieces of debris one cm or

[27] For more information on the Vulnerabilities Triage, please contact the National Communications System, nstac1@dhs.gov.

[28] Satellites in lower Earth orbits can potentially be repaired, although at great cost. Effective technologies are unavailable to repair satellites in higher orbits, including MEO (Medium Earth Orbit) and GEO (Geostationary Earth Orbit).

[29] This kind of attack is likely to be performed only by actors backed by nation-states. Any such attacks could almost certainly be traced and attributed to their origin.

[30] Presenters at the EMP Conference sponsored by EMPACT America, Inc., (http://www.empactamerica.net) stated that the EMP Conference originated after the Starfish nuclear test, which occurred in the Pacific on July 9, 1962, disabled stoplights in Hawaii and destroyed all LEO satellites.

[31] *Orbital Debris Quarterly News*, Volume 11, Issue 2, April 2007.

greater remain in orbit. Scientists estimate that resultant debris from the test comprises over 25 percent of all debris in the LEO regime[32] and that the energy from the collision threw a majority of the debris into long-duration orbits, with lifetimes measured in decades and even centuries.[33]

The near-Earth space environment, particularly LEO, includes orbital debris moving at a high velocity relative to satellites. Today, the DoD uses the SSN to detect, track, catalog, and identify more than 19,000 man-made objects orbiting Earth that are approximately 10 cm or larger. Scientists working with the SSN estimate that more than 300,000 objects with a diameter of one to 10 cm, and billions of smaller objects, remain in orbit. In the 1990s the growth rate of tracked debris decreased annually primarily due to international debris mitigation efforts; however, since 2004 the amount of tracked debris has increased. Debris frequently transits the orbits of hundreds of operational spacecraft and space shuttles, including the human space flight regime, posing risks to current and future space systems. While the majority of debris in LEO is too small for scientists to reliably track and catalogue, it is sufficiently energetic to act as a hazard to satellites.[34]

While the probability of an accidental collision between debris and an active satellite is relatively low, such an event occurred as recently as February 2009, causing the catastrophic failure of a U.S.-licensed Iridium communications satellite. The Iridium 33 communications satellite and a derelict Russian Cosmos 2251 communications satellite crossed paths 790 km above northern Siberia on February 10, 2009, marking the first known instance of satellites colliding in orbit. At a closing speed of approximately 35,400 km per hour, the impact generated 382 pieces of debris from the Iridium satellite and 893 pieces of debris from the Cosmos satellite as catalogued by the SSN. National Aeronautics and Space Administration engineers suspect that the collision may have created thousands of pieces of debris that are undetectable by radar and that may possess enough kinetic energy to damage another spacecraft.[35]

Collisions increase the amount of hazardous debris in the space environment and pose a serious threat to the long-term viability of the space environment for operations, including human spaceflight. The threat of satellite collision continues to grow as the rate of debris production increases. Satellites that collide at lower altitudes (approximately 320 km above the Earth's surface) eventually fall from orbit and burn up upon re-entering the atmosphere. However, objects colliding at higher altitudes may remain in orbit for centuries, posing hazards to other satellites in their paths.[36] Accordingly, avoiding collisions and the creation of additional space debris are of paramount importance.

[32] *Orbital Debris Quarterly News*, Volume 13, Issue 1, January 2009.

[33] *Orbital Debris Quarterly News*, Volume 11, Issue 2, April 2007.

[34] Security Space Index, *Space Security 2008*, September 2008.

[35] At a Congressional hearing held on April 28, 2009, "Keeping the Space Environment Safe for Civil and Commercial Users," Subcommittee Chairwoman Gabrielle Giffords (D-AZ) stated, "One thing is already clear – the space environment is getting increasingly crowded due to the relentless growth of space debris. If the spacefaring nations of the world don't take steps to minimize the growth of space junk, we may eventually face a situation where Low Earth Orbit becomes a risky place to carry out civil and commercial space activities." *Orbital Debris Quarterly News*, Volume 13, Issue 3, July 2009.

[36] Data as of July 15, 2009. http://celestrak.com/events/collision.asp

Mitigation Measures

Collisions between controlled space objects, or between controlled space objects and known debris, can be avoided provided that each operator knows the location of each object and asset, and knows the maneuvers planned by other operators.

The Inter-Agency Space Debris Coordination Committee (IADC) is an international forum composed of 11 Governmental bodies that coordinates and facilitates information exchange on issues and research related to space debris, and documents the progress of ongoing debris mitigation activities. In October 2002, the IADC approved its Space Debris Mitigation Guidelines[37] in which it designated both the LEO and Geosynchronous Earth Orbit (GEO) orbits as protected zones.[38] The document describes space debris mitigation measures, best practices for space debris limitation, and includes mitigation efforts such as limiting the debris produced during normal operations, minimizing on-orbit break-up potential, post-mission debris disposal, and prevention of on-orbit collisions. Following the international process in the Federal Communications Commission's (FCC) Second Report and Order 04-130—*Mitigation of Orbital Debris,* the FCC enacted new rules designed to prevent the creation of additional space debris.[39]

3.1.2 Avoiding Collisions—Space Situational Awareness Information Sharing Between Industry and Government

Operators continuously and accurately track the locations of their own satellites and rely on in-house close-approach monitoring systems to ensure the safety of their fleets. Most operators also incorporate information from the U.S. Joint Space Operations Center (JSpOC) when analyzing potential close approaches between satellites or between satellites and trackable debris. The basic information (referred to as Two-Line Element [TLE] data) used in this process is available to authorized users of the U.S. Government's "Spacetrack.org" website. Operators routinely screen satellites using TLE data, and also exchange data with other operators with near or adjacent satellites during special activities such as satellite relocations and transfer orbit missions. The data exchange usually consists of the latest location information, near-term maneuver plans, transmission frequencies, and contact information for further discussion.

There are drawbacks to the current close-approach monitoring process. In addition to a lack of standards for TLE modeling, TLE data does not have the required accuracy for credible collision detection. An operator that relies on TLE data must increase the calculated collision margin to avoid potential close approaches, therefore increasing the number of maneuvers. Maneuvers based on inaccurate data can waste fuel, shorten the life of satellites, and in some cases can introduce uncertainties that decrease the safety of space operations. In most cases, threats identified using basic TLE data are downgraded after coordination with other operators or further evaluation with more precise orbital data. TLE data also lacks reliable planned maneuver information, which limits the usefulness of data for longer-term predictions since future maneuver information is necessary to properly predict the orbital location of active satellites.

[37] The IADC Space Debris Mitigation Guidelines were updated on September 25, 2007.

[38] "The IADC and other studies have found that fulfilling the additional condition at the end of the disposal phase would give an orbit that remains above the GEO protected region: the eccentricity should be less than or equal to 0.003." Status of IADC Activity presentation, Paris, France, February 7-8, 2008.

[39] Federal Communications Commission Second Report and Order 04-130—*Mitigation of Orbital Debris*, Released June 21, 2004.

Today, operators relying on chemical propulsion systems maneuver about once every two weeks to maintain their orbital position. Accurately predicting the orbital location of a satellite will become more challenging with satellites that employ ionic propulsion systems[40] and are in essence constantly maneuvering.

Adding complexity to this problem is the fact that there is no single standard for representing the position of an object in space. Operators characterize the orbital position of their satellites differently depending on the software used for flight operations. In addition, there is no single agreed-upon protocol for sharing information, and coordinating operators must be prepared to accommodate the practices of other operators. To do this, operators must maintain redundant file transfer protocols and tools to convert and reformat information so that it is consistent with other software systems for computing close approaches. Some operators write their own software tools for monitoring and predicting the close approach of other spacecraft while others contract with third parties for this service. Therefore, separate tools for each operator are necessary to exchange data. The magnitude of the effort to maintain space situational awareness grows quickly as the number of coordinating operators increases. Further, not all satellite companies participate in close-approach monitoring due to lack of financial resources or appropriately skilled technicians.

Since TLE data is relatively imprecise, the U.S. Air Force established the "Interim CFE (Commercial and Foreign Entities) Data/Analysis Redistribution Approval Process" (commonly referred to as the Form 1 Process) for granting operators access to information that goes beyond the basic TLEs. Through this process, operators can request additional information (known as special perturbation [SP] data) on specific close-approach situations. Although helpful, it is cumbersome to rely on the Form 1 Process as an operational tool because it requires advanced notice, which is often impossible to provide in emergency situations, and cannot address many operational issues when time is of the essence.

While the U.S. Air Force Space Command (AFSPC) led development of the CFE Program, the MAWG served as the conduit for Government interaction with the COMSATCOM industry. The NSSO established a Flight Dynamics Task Force which gathered information and data requirements and provided the results to AFSPC so they could understand industry's concerns and information requirements to support commercial space flight safety issues. The MAWG continues to support industry engagement with the government as USSTRATCOM assumes operation of the CFE program from AFSPC.

Data Center Proposal

In response to the recognition that better and broader inter-operator information sharing is desirable and to augment the services available from the current TLE-based DoD CFE Program,[41] a number of satellite operators recently began a broad dialogue on how to best ensure

[40] Ionic propulsion yields relatively low thrust compared to chemical propellant, and thus limits emergency maneuver command capability.

[41] CFE was a pilot replacement for the NASA program sharing orbital data with non-U.S. Government users from 1960s-2003. The Air Force Space Command executed the CFE Pilot Program under the authority granted by Congress in November 2003 (FY04 NDAA) and extended (in FY07 and FY09) to September 30, 2010. Since 2003, the CFE program has provided registered users (documented by an on-line registration agreement) access to basic

information sharing within the satellite communications industry. The international satellite community is discussing forming a Space Data Association (SDA), which would be an interactive repository for commercial satellite orbit, maneuver, and payload frequency information. The principal goal of the SDA's Data Center would be to promote the safety of space operations by encouraging coordination and communication among its operator members. Satellite operators would maintain the most accurate information available on their fleets in the Data Center systems, augment existing TLE data with precise orbit data and maneuver plans from the operator's fleets, and would retrieve information from other member operators when necessary. The Data Center would also allow operators to:

- Perform data conversion and reformatting tasks allowing operators to share orbital element and/or ephemeris data[42] in different formats;
- Adopt common usage and definition of terminologies;
- Develop common operational protocols for handling routine and emergency situations; and
- Exchange operator personnel contact information and supported data protocols.

As the Data Center gains acceptance, it could perform additional functions such as close-approach monitoring tasks currently being conducted by operators. In this phase, operators could augment U.S. Government-provided TLE data with more precise operator-generated data to improve the accuracy of the Data Center's conjunction monitoring and provide a standardized method and focal point for operators to share information and facilitate communications between satellite operators and U.S. and non-U.S. governments. In the early stages, TLE data from the CFE Program and/or other Government programs would still need to supplement information on non-operational space objects. Additionally, U.S. Government or non-U.S. government support would still be required when precise information is required to conduct avoidance maneuver planning.

Details on the implementation of the Data Center, services to be provided, usage policies, structure of the organization, and by-laws have yet to be determined and would ultimately require agreement among the member operators. The development of a Data Center could provide new visibility and awareness of the space environment, allow satellites to be flown in a safer manner, and reduce the likelihood of an accidental international incident in space.[43]

orbital data via an online web site (www.space-track.org). Further, CFE offered additional limited collision avoidance support using specific request procedures for a limited set of users pursuant to bilateral agreements.

[42] Ephemeris data is a set of parameters used to accurately calculate the location and describe the orbital path of a satellite at a given point in time.

[43] The prototype Data Center expanded quickly, and today commercial and civil U.S. and non-U.S. government satellite operators participate and regularly contribute data from over 150 satellites in GEO orbit. The participating operators receive daily close-approach alerts when approach-distances and conjunction probabilities fall below certain thresholds, and a daily neighborhood watch report showing the projected separations of satellites that are flying in an adjacent control box. The participating companies provide ephemeris data in the reference frames and time systems generated by their flight software, and the Data Center performs the transformation and reformatting to a common frame for close-approach analysis. This greatly simplifies efforts and reduces the burden on individual operators, and thus encourages participation. A strict data policy has been put in place to ensure data privacy. The Data Center may not redistribute the data received from owners/operators without the prior approval of the owners. While there is still significant work left to refine the process, the initial results from the Data Center prototype are very promising.

Government Improvements to Space Situational Awareness
The Commander of the Air Force Space Command has assured commercial satellite service providers that improvements in the Air Force satellite and tracking network will enable the Air Force to more effectively provide early warning of any possible conjunctions. Improvements to the ground optical and radar sensors, the JSpOC, the satellite tracking network, and the introduction of the Space Based Space Surveillance system will provide major improvements to the system in the future. Hosted Government payloads/sensors on commercial satellites could provide a "neighborhood watch" type of space situational awareness and enhance the overall network.[44] Operations procedures are also being established to ensure better notification of all satellite operators. These actions show that DoD has made space situational awareness and data sharing an important, near-term initiative.

3.1.3 The Ground Environment

Ground segment components of any communications infrastructure are among the highest-risk targets of physical attack, destruction, or incapacitation because conducting an attack on such facilities requires little expertise or expense. An attack could significantly disrupt satellite communications services; however the impact would vary based on the functionality of the facility and the existence of back-up facilities. Because the cost to establish and maintain the ground segment is less than the cost to develop and deploy space components, most operators improve their reliability on the ground with dissimilar redundancy. The loss of terrestrial satellite facilities due to a natural disaster or intentional attack would disrupt service to customers temporarily, but since the satellite in space would remain unharmed, service could be rapidly reconstituted if an appropriate back-up plan is in place.

Mitigation Measures
The NSTAC found in response to its questionnaire that the satellite industry utilizes a range of standards-based physical security protection techniques to mitigate against a man-made attack or natural disaster. Satellite NOCs, SOCs, and TT&C ground stations generally maintain 24-hour guarded access, security fencing, external lighting, registration and clearance of visitors, and security cameras to monitor the area to dissuade man-made attacks, including capture of a ground station. To combat the results of natural phenomena, providers employ back-up facilities; construct facilities outside of disaster-prone areas; plan for antenna stow methods or protective procedures; and maintain fire detection, flooding, and de-icing procedures. Most commercial providers also maintain back-up facilities and auxiliary power sources in the event of a man-made attack or natural event. However, auxiliary power availability is limited by on-site fuel availability, generally ranging from a minimum of 24 hours to a maximum of 30 days. Further, facilities are generally not constructed to withstand a nuclear detonation, electromagnetic pulse (EMP) and biological attacks, or radiological fallout. Similar to other facilities, satellite operators have established personnel security procedures including background checks and pre-employment screenings, employee badges, logged entry and exit, and on-site security guards.

Satellite ground stations and control stations are not at any greater risk than similar facilities of other terrestrial communications providers. This is because most large operators employ best

[44] The NSTAC also supports U.S. Government plans to upgrade the Space Fence, a radar system that detects objects in orbit over the U.S. that was originally deployed in 1961.

practices such as the use of redundant, geologically diverse facilities for critical functions. Therefore it is unlikely that a single physical event would simultaneously impact both a primary and back-up Earth station. Similarly, extraordinary events, such as the effects of an EMP attack, would be partially mitigated due to the diversity of ground stations. In response to the questionnaire conducted to support the Core Assurance effort, 100 percent of respondents stated that NOC, SOC, and TT&C sites are connected by multiple communications links that provide redundancy and physical path diversity. Additionally, ground stations utilize prevention and recovery techniques to mitigate risk, including buffer zones; redundant circuits between sites; and robust security systems to protect NOC, SOC, and TT&C sites from attack.

3.2 Access & Control Threats

Communications providers need to be able to control and monitor their network infrastructure to reliably deliver services to customers. Satellite service providers must control their satellites and associated payloads in space in addition to controlling their terrestrial network elements, including routers, switches, modems, and authentication servers. Given the very high cost and amount of time required to design, build, and launch the satellite into orbit, operators enact measures to ensure that they are the only parties able to remotely command their systems and that third parties cannot interfere with operations.

3.2.1 Satellite Command Links (Command Link Spoofing and Purposeful Interference)

Satellites in orbit are controlled remotely by commands generated at one or more SOCs and are transmitted by radio to the satellite. Most satellites use command receivers that can see the visible Earth, allowing for flexibility in positioning ground facilities to command the satellite. Importantly, these command links differ from those used to transmit customer services, thus there is no risk that a customer could remotely control a satellite. While, as discussed below, SOC operations are generally well-secured on both a physical and cyber level, it is important that the satellite’s RF command system be designed to allow only the authorized user—the satellite operator—to control the satellite. Most satellite industry owners and operators experience some form of cyber threat activity to varying degrees, such as probes into operational networks from the Internet and interference (unintentional and, very rarely, intentional). To maintain the security of the SOC, there are two risks that must be mitigated: (1) an adversary remotely introducing a satellite command; and (2) the satellite operator losing the ability to transmit commands or receive telemetry from the satellite.

Mitigation Measures

Most satellite operators mitigate satellite command link threats by using a combination of the following techniques:

- **Encryption**: Use of encryption systems onboard the satellite RF command receiver and resident in the ground systems to preclude an attacker from sending an unauthorized remote command to the satellite;
- **Deaf Satellites**: Satellite RF command receiver design that requires very high power transmissions and associated large transmission antennas before the satellite can hear the satellite command. An attacker gaining access to these large, immobile facilities is non-trivial;

- **Carrier Lockup**: Satellite system design that continuously "phase locks" a satellite command receiver to the satellite operator's ground transmissions, preventing the insertion of commands from other ground stations while the primary ground station is in operation;
- **Uniqueness**: Each satellite command decoder uses a unique address to ensure that commands are received only by the intended satellite. Each satellite's command database is customized for the specific spacecraft, thereby reducing the chances that an adversary would be able to reverse engineer the specific commands used to control a specific satellite;
- **Autonomy**: Satellite system design that allows the satellite to operate autonomously for long periods of time without receiving commands from the satellite operator. Autonomy is utilized in cases of command link RF interference, and to reject or recover from dangerous commands unless the command is confirmed as authentic;
- **Diversity**: Most satellites generate two independent telemetry streams, mitigating attempts to interfere with telemetry reception. Operators also use multiple, geographically diverse ground stations to more reliably transmit commands and receive telemetry information; and
- **Out-of-Band Commanding**: Satellite command receivers are tuned to frequencies that are not shared with customer traffic or terminals.

Since 2007, satellite operators have increasingly specified satellite command uplink systems that employ cryptographic implementations, including those approved by the National Security Agency (NSA) to encrypt the command transmissions, which effectively eliminates the risk of a remote RF command injection attack while the satellite is operating in encrypted command mode.[45] Such systems are required by CNSSP 12 when commercial satellites are used to carry national security information, and since 2008 the DoD has included this requirement for commercial Fixed Satellite Service operators providing service under its DSTS-G contract.[46] The NSTAC was unable to determine the extent to which CNSSP 12 requirements are actually enforced. The number of legacy communications satellites in orbit that are technically incapable of encrypting command traffic continues to decrease as older satellites reach their end of life and are replaced. Satellite operators that totally fail to protect their satellite command systems from intrusion create the risk that they may lose control of the satellite in the face of a capable, determined adversary. If an adversary were able to successfully execute such an attack, it would be difficult to attribute, thus limiting responsive options.

3.2.2 Operations Center (Satellite Operations Center and Network Operations Center) Vulnerabilities

As discussed above, the SOC is the center where command, control, and monitoring of the satellite occurs. If the SOC is unable to reliably control the satellite in space or receive accurate telemetry to monitor its health and location, service availability may be compromised. The NOC

[45] The proper design, implementation, and validation of a cryptographically secure command system is nontrivial. Satellites using other than NSA-approved implementations, for example, should use cryptographically secure implementations that include the use of properly seeded random numbers using a commercially vetted random number generator to deter attacks based on deterministic patterns.

[46] Satellite operators with non-U.S. operations face special challenges in using NSA-approved crypto systems, such as Caribou, due to stringent export control and U.S. Government oversight of the ground-based encryptors that must be used with these systems. Development of approved alternatives may foster adoption of encrypted command systems by more operators.

is responsible for configuration management and network monitoring of traffic on the communications operator's network; this often includes managing the underlying RF carriers on the satellite network.[47] Like the SOC, the primary threat to the NOC is an individual seizing control of network infrastructure or compromising the integrity of the control network, which may result in service disruptions.

Since the mitigation measures for both the SOC and NOC are highly similar, this report considers the SOC and NOC together as operations centers. Notably, risks and mitigation measures for these operations centers are identical to those best practices employed by terrestrial communications carriers, and the fact that satellite technology is used in the underlying network creates no special risks or vulnerabilities.

Mitigation Measures

To mitigate operations center vulnerabilities, providers have implemented more intrinsic controls around those systems. Malicious actors do not require physical access to the satellite or the terrestrial network components. They require only access to the control center systems, which can occur, for example, via a compromised control center workstation.

To properly protect operations centers, one must implement: (1) physical controls; (2) network layer controls; (3) applications security controls; (4) system-level controls; and (5) redundant or back-up facilities. Proper physical controls include guards, gates, staff background checks, identification (ID) badges, and continued auditing of physical security systems to prevent unauthorized access. Networks that operate across wide areas or in third-party facilities generally employ strong cryptographic controls to ensure the confidentiality and integrity of transmitted and received information. Especially sensitive networks may be "air gapped" and not interconnected at all with other networks. Remote access sessions, when authorized, are carefully secured. Additionally, general systems controls ensure that the correct security countermeasures are in place to stop worms and viruses, and have the proper network access controls including gateways, firewalls, and hardening of systems and network infrastructure so that only authorized personnel are granted access to the network.

Application security controls include authentication and authorization, well-defined operating procedures, and audit controls. Two-factor authentication should be used—not only a log-in and password, but also a token—for entry into the system. Audit controls such as monitoring and logging give authorized personnel visibility into activities that occur throughout that commanding system, and can provide a useful record to develop mitigation strategies to stop future malicious activity. A good log will show who initiated a malicious command, at what time, and through what method. Further, one can write code that allows for visibility into what is happening to the satellite by logging the commands of each person on the network and identifying how an individual affected the satellite.

[47] Many satellite operators use distinct control centers to manage the physical layer (the radio-frequency loading) of a satellite system, and the network layer of derived services (e.g., the IP network traffic flowing over the satellite). These respective functions are sometimes known as payload management and network management.

System-level controls include endpoint security measures (anti-virus, spyware, local/host-based firewalls, host-based intrusion prevention systems [IPS]) use of Public Key Infrastructure, and auditing and monitoring at the system level.[48]

Operations centers controlling network traffic also require network access control systems, including firewalls and router access control lists, monitoring, and network-based IPSs. To mitigate human threats, the NOC requires real-time visibility controls for actual network traffic entering the terrestrial data center to allow operators to view information transiting the network and to take immediate action to protect network availability in case of a physical or cyber attack. Just as with application security controls, operators maintaining good logging practices will be able to determine who entered commands, when the commands were entered, and how this affected the network infrastructure.

Finally, the private sector relies on a variety of initiatives to help safeguard the health of the network. In addition to the Data Center initiative discussed above, operators use professional outreach, networks, and publications; collaboration through industry-to-industry and industry-Government working groups; and anti-malware programs and firewalls to protect networks from the threat of cyber attacks. Satellite owners, operators, and manufacturers employ dedicated individuals and teams within their respective organizations that deal specifically with cybersecurity threats. Additionally, many satellite owners and operators maintain redundant or back-up facilities for SOCs, NOCs, and TT&C sites, as discussed above in Section 3.1.3. Backup facilities are regionally diverse, active, and regularly tested to ensure that operators can continue to provide service in the event of a physical or cyber attack.

3.3 User Segment Threats

Ultimately, satellite networks rely on radio transmissions between ground stations and end user terminals to create communications pathways capable of supporting network services such as video distribution, voice, or IP over the satellite. Regardless of network type, network operators have several classes of cyber threats in common, including viruses, worms, botnets, and denial of service attacks. Networks using satellite user links are equally as susceptible to these threats as is any other terrestrial network. Satellite network operators use the same tools, techniques, and processes to detect and address network-level threats as any other operator. Because these network-level threats and mitigation techniques are well-known to the NSTAC and the network security community, this report does not address them. However, the large size of a typical satellite beam coverage area (footprint) increases the vulnerability of satellite networks to interception or a purposeful interference (PI) denial of service attack as compared to other modes of communication.

3.3.1 Unintentional Interference and Purposeful Interference

As the capability of both state and non-state actors to interfere with satellite communications continues to increase, the most vulnerable network components are the underlying RF communications links, which are susceptible to both intentional and unintentional RFI.[49] Satellite communications links require specific electronic protection measures to safeguard their

[48] See, for example, NIST SP 800-53. August 2009.

[49] Chandler, Captain Roy, "Total Force 'RAIDRS' keep high frontier secure," Air Force Times Online, January 2008.

utility against denial of service attacks. Continued occurrences of both unintentional and intentional PI demonstrate the vulnerability of satellite communications to these threats. Moreover, the significant security issues and financial costs that result from interference show the adverse effect that relatively low-cost, low-technology threats can have on the security of space operations and cyber operations.[50]

Sources of Unintentional Interference or Purposeful Interference

As in 2004, both uplink and downlink interference remains a threat to the satellite industry. Although instances of PI have appeared on a more frequent basis, PI remains exceptionally rare and is unlikely to be confused with unintentional interference over a long period of time. Both PI and unintentional interference affects service to customers by interfering with the reliable transmission or reception of the wireless signals used in the satellite network. Depending on the design of the satellite network and the source of interference, service disruptions can occur locally or over a large area.

PI is considered a temporary denial of service threat than can last for hours, days, weeks, or months. Once the PI ends, normal network operations will resume. An actor initiating an uplink interference attack will insert a signal into the satellites' uplink transponder, which can lead to a denial of service condition throughout the beam area served by that satellite. Downlink interference can lead to a more localized disruption in satellite services as an unwanted, interfering signal is directed in Earth terminal receivers, masking the reception of the desired satellite signal in an area within line of sight of the jammer. PI can be accomplished without a significant investment; well-financed actors can create larger-scale effects.

There are several sources of satellite communications interference: (1) human error; (2) adjacent satellite interference; (3) terrestrial interference; (4) equipment failure; and (5) PI.

- **Human Error**: Most interference is due to human error, or user interference. User interference is usually accidental resulting from terminal operator error due to inadequate training, poor system configuration, or inferior terminal design. These interference types are usually relatively easy to identify, and can be resolved relatively quickly. Cross polarization, also known as Crosspol, is a type of radio frequency interference experienced by COMSATCOM providers and users. Crosspol is usually caused by transmission of incompatible modulation types (analog modulation formats such as FM TV) in the opposite polarization to digital services on the Crosspol, or by poorly aligned antennas in bursting networks. Crosspol can usually be attributed to a lack of user training, inexperience, or poor uplink terminal access procedures.
- **Adjacent Satellite Interference**: Adjacent satellite interference is generally accidental and results from poor inter-system coordination or user error in antenna pointing. Interference caused by adjacent satellites is becoming more prevalent as the geostationary arc becomes more crowded. Mitigation requires good planning and correctly specifying and deploying user terminals; for example, orienting the terminals to point to the correct satellite and ensuring that the terminals use sufficiently narrow, high-performance beams.

[50] Security Space Index, *Space Security 2008*, September 2008.

- **Terrestrial Interference**: Terrestrial interference can be caused by a variety of means, including existing terrestrial microwave systems, new microwave systems that have commenced service following deployment of the satellite, and civil or military radar systems used on land, sea, and air platforms. Inter-system frequency coordination procedures, pursuant to the International Radio Regulations, are designed to address this issue.[51]
- **Equipment Failure**: Equipment failure can cause uncontrolled and unwanted radio emissions. Poorly designed terminals, instead of shutting down in their failure mode, can continue to transmit signals, causing interference. Equipment failure can be managed through better design, planning, systems management, operator training, and maintenance.
- **Purposeful Interference**: PI can be seen as geopolitically motivated and exceptionally rare; however, its effects can be significant. In the cases of PI observed over the past decade, an important step to mitigate the issue includes rapidly locating the source of the jamming signal(s) so that appropriate measures can be initiated at the government-to-government level to resolve the situation, such as the use of International Telecommunication Union procedures or bilateral approaches. Jammers can employ a number of strategies, including mobility, to thwart mitigation.

Mitigation Measures

Overall, there are a number of means to mitigate RFI, including user training and certification, identifying and eliminating the interference source, using filters, and grounding and shielding equipment.[52] The use of filters and physical shielding may be useful in rejecting strong nearby signals that can be found at satellite terminals, but are ineffective against PI. Terminal operator equipment training and proper system operation is paramount to reducing unintentional RFI.

Traditional communications satellite systems employ large footprints that may cover wide regions or even continents. For this reason, satellite networks may experience RF and uplink interference issues that are greater in geographic scope than those experienced by terrestrial wireless networks. Low-power or infrequent jammers may seek to distort the user's data in order to reduce effectiveness or trust in the system; this can be difficult to differentiate from unintentional interference. At higher powers, a more overt jammer can saturate key satellite components so that the desired signal is essentially eliminated altogether. Not all military and commercial communications satellite systems are intended to provide complete protection from RFI; robust protection measures remain primarily the domain of certain specialized Government systems such as MILSTAR (Military Strategic and Tactical Relay [satellite]). Satellite systems can employ a combination of antenna beam control (narrow spots, beam steering, or nulling) and spread spectrum techniques to reduce jammer susceptibility. The most effective forms require elaborate antennas and onboard processing, well beyond what can be economically justified in a commercial environment. The Government could enhance commercial satellite mission assurance through targeted funding to implement these measures outside of specialized Government systems.

[51] For more information see: http://www.itu.int/en/pages/default.aspx
[52] Burrell, James, *Disruptive Effects of EMI on Communication and Electronic Systems*, April 2003.

3.3.2 Commercial Detection, Characterization, and Geolocation of Interference Sources

Commercial satellite operators providing leased transponder services generally manage the RF carrier assignments on their payloads using 24x7 operations centers linked to a distributed network of communications status monitoring (CSM) nodes to monitor RF spectrum usage in each satellite beam coverage area. Operators use these CSM systems to monitor, record, and archive RF activity, perform signals analysis, audit customer use, and identify unauthorized system use. CSM systems allow for the identification of interference, and include automatic alarms when interference is detected, allowing operators to promptly initiate mitigation procedures.[53]

Mitigation Measures

Typical mitigation measures include signal analysis, customer audit, and alerting. Geolocation is an advanced mitigation measure that, in many cases, allows satellite operators that have access to the technology to rapidly identify the geographic source of an interfering signal by using advanced signal processing techniques coupled with known information.[54] Geolocation depends on a number of factors including: (1) adjacent satellite(s) with similar transmission characteristics; (2) access to precise information on satellite location and velocity (ephemerides); and (3) reference emitter signals and transmitting Earth station locations.[55] Given the need to rely on adjacent satellite systems, cooperation and data sharing among satellite operators and between satellite operators and the Government is essential for the adoption and evolution of effective geolocation technologies. The commercial satellite industry participates in numerous RFI reduction groups and is exploring additional ways to better share information. Further, the Data Center discussed in Section 3.1.2 could provide updated and more accurate satellite ephemeris data that would assist in using commercially available location systems.

3.3.3 Industry Efforts to Reduce Radio Frequency Interference

Industry is working to advance initiatives to reduce RFI. For example, 11 satellite operators are already working together on a project called the "Satellite Operators' RFI Initiative" that is meant to respond to concerns expressed by customers regarding the increase in satellite RFI incidents and the impact these incidents have on the quality of commercial satellite services.

Each year, thousands of satellite RFI incidents are reported. Over the years, satellite operators have developed informal agreements and deployed new technologies to attempt to address this issue. With respect to interference of a U.S. Government service, satellite operators cooperate and resolve those events directly with the Global SATCOM Support Center (GSSC) in Colorado Springs, Colorado. However, these informal agreements have not kept pace with the growth of

[53] Digital signal processing techniques allow a high degree of automation in carrier monitoring, but, given the scope of their networks, satellite operators find it cost-prohibitive to continuously monitor all signals.

[54] These technologies use the presence of the interfering signal in two satellites to generate a differential frequency offset (due to different satellite velocities) and differential time offset (due to differences in the transmission path length of the signals taken through the two satellites) to create an ellipse on the Earth that indicates the likely source of the interfering signal.

[55] The accuracy of the result is a function of the capabilities of the system and the quality of the data: satellite ephemerides accuracy, reference emitters, system measurement accuracy and stability, processing power, signal levels, size of the interfering/operating antennas, nature of the interfering signal, and the geometry of the interference event. The time needed to perform a measurement depends on the availability of input data, operator experience, and the nature of the interference event.

the problem, and the combination of more satellites in the sky and more terminals on the ground is raising new operational challenges.

As a result of the growth of the commercial industry, as well as the corresponding increase in demand for new orbital locations and radio frequencies, the physical distance between satellites has decreased. This new proximity has increased the problem of adjacent satellite interference. In today's marketplace, there is a demand for smaller and more mobile terminals that require increased uplink power, which in turn increases the likelihood of interference.

As the terminal industry has grown and new suppliers have entered the marketplace, it has been difficult to monitor the quality of some products. At the same time, rapid growth in demand has left some satellite customers, including Government users, with no easy access to training. Industry records clearly indicate that "operator error" of user terminals remains one of the most significant causes of satellite interference. Concern over these issues has motivated satellite operators to launch the Satellite RFI Initiative, which is focused on accomplishing three major objectives:

- **Support Standardized Training/Certification**: Training is an essential element of good satellite operations. With the expansion of the industry and increase in competition, the satellite industry's commitment to training its antenna installers and uplinkers has wavered. Operators participating in the initiative seek to gain support for standardized training and, where appropriate, institute certification programs to ensure compliance with industry best practices. Operators are also exploring ways to provide training resources to specialized communities such as Government users.
- **Endorse Carrier Identification Technology for Terminals**: Carrier ID technology would help to identify malfunctioning or poorly maintained equipment by imbedding information such as location, contact details, and equipment data within the satellite signal. Alternatively, a coded identifier could be specified for Government operations requiring higher levels of security. For the carrier ID to be successful, satellite equipment manufacturers would have to include the technology as a standard feature in their equipment. As part of the Satellite RFI Initiative, satellite operators will work with major manufacturers to try to build consensus regarding the inclusion of this technology. In this area, there are opportunities for the Government to encourage the adoption of this approach by requiring controls on future Government acquisitions.
- **Build Data Sharing Between the Satellite Operators**: The Satellite RFI Initiative seeks to formalize, standardize, and, where possible, automate the process of sharing information about interference events. To identify the source of an interference event using geolocation technologies, operators need to know a number of elements, such as precise satellite location and configuration information and known uplink sources (often referred to as reference emitters). This data could be included in an RFI Database and routinely shared as part of an interference alert network; this concept is being actively explored by operators forming the Data Center discussed in Section 3.1.2.

3.3.4 U.S. Government Initiatives to Address Interference

Global SATCOM Support Center
USSTRATCOM's GSSC provides operational SATCOM management and support for global, national, and theater Government users of military and commercial SATCOM. The GSSC maintains and disseminates global SATCOM situational awareness, which includes mission planning, constellation loading, network utilization and optimization, anomaly/EMI resolution, network configuration support, and international partner coordination. It is the Government's lead for resolution (detection, characterization, and geolocation) of acute EMI, and it supports resolution courses of action for chronic EMI and unauthorized use of satellite resources.

Government EMI/RFI Detection, Characterization, and Geolocation Resources
DoD continues to develop and field systems to detect, identify, geolocate, and report on sources of interference from both unintentional and deliberate attempts to interrupt SATCOM. Eagle Sentry is an example of a system that has already been deployed to three separate operational locations worldwide. The U.S. Air Force's Rapid Attack Identification Detection Reporting System (widely known as RAIDRS) is in development with expectations to have the system fully operational by 2011. The level of proposed operational interaction and information sharing between Government systems and the commercial satellite industry remains unclear, but such systems could become a useful tool to help support commercial operator efforts to address interference.

Purposeful Interference Response Team
In FY 08, the Purposeful Interference Response Team (PIRT) was created at the request of the National Security Council. USSTRATCOM chairs the PIRT, as the U.S. Government lead for space operations and the operators of the primary U.S. Government 24-hour operations center for space situational awareness. The PIRT is an interagency[56] coordination group designed to bring together SMEs from across the U.S. Government to evaluate reports of suspected PI that impacts U.S. Government space systems, commercial and foreign systems providing services to the U.S. Government, and other U.S. commercial and allied space systems and services of interest to the U.S. Government. PIRT serves as an investigative and coordinating body to ensure all relevant U.S. Government agencies have access to the same information and key analytical documents to develop resolution options, and formalizes and facilitates existing processes and relationships.

USSTRATCOM chairs PIRT with the goals of:

- Serving as the single focal point for prompt notification to its members of suspected PI events and for ongoing consolidation and dissemination of information concerning suspected PI events; and

[56] PIRT core membership currently includes: DoD, Department of State, Department of Commerce, DHS, Department of Transportation, the Director of National Intelligence, and the Federal Communications Commission. The National Security Council, Director of Space Policy, and the Office of Science and Technology Policy's Senior Policy Analyst for Space participate as observers. The PIRT Charter also allows for Conditional Members in cases where an agency operates an affected space system, has contractual or regulatory authority over an affected space system, or can provide specialized expertise relevant to a specific event.

- Maintaining unity of effort and consistency of message with the owner/operator of the affected system, once an event has been determined to warrant convening a PIRT support.

While the authority to direct agencies to take specific actions in response to suspected PI remains in the hands of the various agencies and departments, PIRT maintains awareness of suspected PI events, monitors suspected PI events, coordinates and integrates the development of response options, and provides recommendations based on its evaluations. In order to maintain readiness and to ensure consistent treatment of all PI events, the PIRT meets quarterly to discuss current threats, potential scenarios, and potential response options. The PIRT schedules semiannual exercises, and works with planners from core member agencies to develop response plans for potential inclusion in various interagency contingency plans.

3.3.5 Communications Security

COMSEC refers to measures and controls taken to ensure the authenticity of telecommunications; it includes cryptosecurity and transmission security (TRANSEC).[57] Like terrestrial operators, satellite network operators generally provide a transmission path that customers are responsible for securing from interception.[58] TRANSEC methods commonly used to help protect transmissions from interception and exploitation include techniques such as frequency hopping, spread spectrum, and secure time diversity. Bandwidth optimization and compression technologies are also used on the ground-based segments of both commercial and Government satellite networks for this purpose.[59] The NIST defines Federal Information Processing Standard (FIPS)-140-2, which sponsors a certification process for commercial companies wishing to offer certified products containing TRANSEC for sensitive-but-unclassified traffic.[60] Several companies either currently offer FIPS-certified products used in satellite networks, or are in the process of obtaining certification.

3.4 Emerging Technology Issues

Commercial satellite systems are being enhanced to add capacity and to better support commercial and Government needs, including national communication systems and NS/EP. Recent deployments and continued development by the satellite industry involve emerging

[57] TRANSEC is defined in the National Information Assurance (IA) Glossary. CNSS Instruction No. 4009. Revised June 2006. TRANSEC for commercial systems is generally limited to measures that hide the signaling and control information on the satellite links.

[58] Different encryption technologies use widely available commercial implementations and algorithms (including IP security virtual private networks security and Government approved AES-256 based encryption) or bulk traffic encryption implemented using Government-furnished cryptosystems such as NSA Type I.

[59] A satellite communications system for the DoD is typically required to meet COMSEC and TRANSEC requirements. COMSEC requirements can be met in an IP-based network with HAIPE (High Assurance Internet Protocol Encryptor: a Type 1 encryption device that complies with NSA's HAIPE IS [Interoperability Specification]) encryption devices, but only protects the user data from cryptoanalysis techniques. TRANSEC requirements protect transmissions from adversaries by reducing the possibility of interception and detection; without such measures, a COMSEC-only encrypted satellite transmission may still give critical information to an adversary. In addition, DISA is advancing the adoption of NSA-approved TRANSEC as part of the Joint IP Modem program, which is equivalent to NIST FIPS certification in that it is designed to support sensitive-but-unclassified traffic.

[60] TRANSEC is designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. The goals of TRANSEC include low probability of interception, low probability of detection, and resistance to jamming.

technologies such as multiple spot beams, use of relatively undersubscribed spectral bands, regenerative payloads, and adaptive resource allocation. The next generation SATCOM systems may also include additional networking capabilities such as digital processing payloads.

The next generation SATCOM capability is now being deployed with significantly higher capacity, broadband data rates, peer-to-peer connectivity patterns, flexible coverage areas, and dynamic resource allocation on demand. With the expanded support for IP packet quality of service (QoS), SATCOM has now entered a new era of higher throughput and bounded user transmission delay, even for the GEO. These systems now have the QoS and capacity to support high definition video conferencing, which is fast emerging as an effective approach for collaborative decision making. These advanced capabilities have been enabled with a combination of multiple spot beams in the uplink and downlink, packet processing, and/or bandwidth-on-demand functions that are all implemented within the satellite.

3.4.1 Next Generation Satellite Communications Technologies

Unlike early satellites, which tended to employ a single large beam covering continental size areas, new generations of satellites now provide multiple spot beams, which can reuse the allocated spectral band multiple times, as shown in Figure 3 (next page). This spectral reuse adds significant capacity to the satellite system. These uplink and downlink beams can be hard-wired statically at the satellite design time, have configurable connectivity, or use a packet processor to route or switch for more-flexible packet-by-packet level connectivity across all beams, including beams on different spectrums (C, Ku, etc.) with different waveforms and access speeds.

The use of a packet processing function in the satellite requires a regenerative payload that includes demodulation and decoding functions to extract data packets from the waveforms, which are then routed or switched based on their destination address to the respective downlink beams (where they require coding and modulation before transmission). Unlike a bent-pipe (transponded) satellite, a regenerative satellite payload essentially becomes a networking node. The addition of a packet processing function within the satellite enables a scalable full-mesh operation among all beams, as shown in Figure 3, where a small terminal can directly communicate with any other terminal without being routed through a hub. Full-mesh is useful since the GEO satellite propagation delay for a hop[61] is at least 250 milliseconds and a two-hop operation will compromise high fidelity real-time interactive communication. The addition of these new networking functions on the satellite can introduce vulnerabilities similar to those experienced by comparable terrestrial network nodes. As a result, new satellite networking functions need to be supported by a comprehensive security architecture that brings all segments (satellite, ground control, and terminals) into its fold.

[61] A hop is a communications signal that travels from the ground to the satellite and back to the ground.

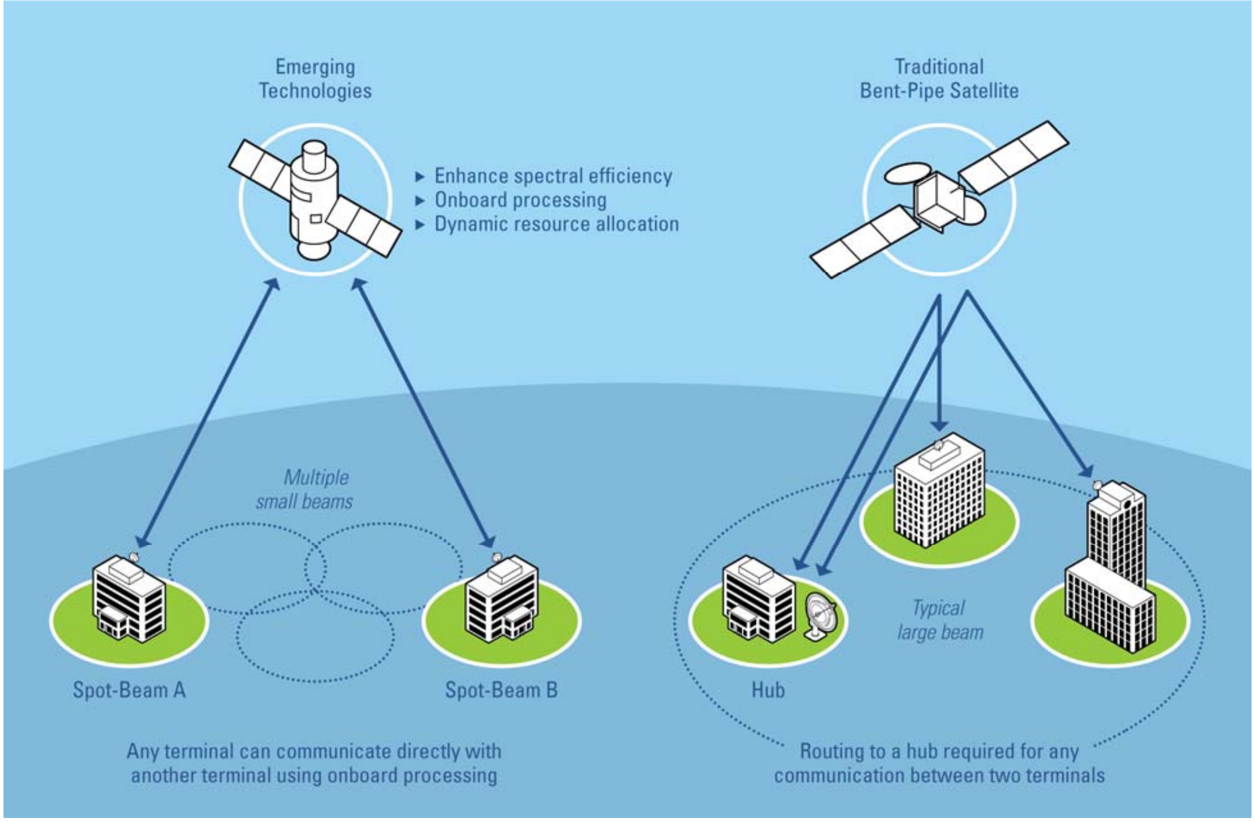
Emerging Technologies
▸ Enhance spectral efficiency
▸ Onboard processing
▸ Dynamic resource allocation
Traditional Bent-Pipe Satellite
Multiple small beams
Spot-Beam A
Spot-Beam B
Typical large beam
Hub
Any terminal can communicate directly with another terminal using onboard processing
Routing to a hub required for any communication between two terminals

Figure 3 Large Capacity Possible With the Use of Multiple Spot Beams and Full Mesh Connectivity Enabled by Packet Processing on a Regenerative Satellite

3.4.2 Multiple Spot Beams

Besides augmenting capacity with frequency reuse, multiple narrow beams have some resilience to RFI, because an interfering signal from any non-local (not in the same uplink beam) site will be attenuated by the satellite receiver subsystem for a beam. Since it is easier to locate (and silence) the RFI source that is located closer to the jammed site, the multi-beam satellite systems have the inherent advantage compared to the traditional single (or large) beam satellites where the RFI source could be anywhere in a larger geographical area. Even without any regenerative capability, the next generation multi-beam satellites would provide large capacity, increased resilience to RFI, and adequate support for the hub-and-spoke[62] satellite network topology that has served the hierarchical organizational structures and consumer Internet access well. Here all processing is done at the headquarters or large Internet websites, and the remote branches or consumers do not directly communicate with each other over the satellite and instead are routed via a hub.

3.4.3 Security Measures for Regenerative Satellite Systems

The centralized hub-and-spoke approach, though applicable for most scenarios, may not be adequately suited for an increasingly complex world with intricate peer-to-peer communication patterns across different hierarchies. For example, during a rapid emergency response, remote sites often must communicate directly with each other. The ability to use these regenerative

[62] A network topology where multiple devices are connected to a central connection point.

satellite IP packet QoS capabilities are also vital to an end-to-end interoperable networking for supporting emergency telecommunication service for voice (and in future video) calls. For such full-mesh connectivity, the regenerative satellites with better link margins and lower delay mesh transport are needed. With the satellite itself becoming a networking node in a regenerative system, this leads to the possible introduction of new vulnerabilities that deserve further security assessment and protective measures. This calls for careful analysis of hardware and software implementation of satellite network node functions for the life cycle of the satellite.

Satellite-based packet processing may be implementable in hardware and/or software, depending upon the required flexibility, capabilities, and interoperability. Higher layer functions and protocols typically require a substantial amount of software that needs to be securely developed and maintained for continued interoperability with other networking nodes. Use of COTS software and upgradeable hardware allows for the regenerative system to take advantage of the extensive security and networking functionality, as well as the research and development available to terrestrial networks today and in the future. The introduction of a digital processing capability in the satellite enables additional security measures in the regenerative systems. For example, the satellite payload demodulators can count the transmitted packets, which can then be correlated with aggregated counts from terminals to detect any fraudulent or malicious behavior. A hardware-based terminal security access module can allow the build up of a secure system architecture, including terminal and satellite communications. A hardware-based security system can also be used to "boot-strap"[63] secure terminal registration and support authentication and encryption of higher layer (such as IP) control, management, and user data transport.

While improving system performance, the introduction of regenerative systems can raise a new class of issues during a deliberate attack, including the potential for denial of service attacks on satellite networking nodes and the loss of signal information needed for geolocation of jammers. If the use of regenerative systems expands, these will require further study to mitigate.

3.4.4 Commercial Implementations

Since the publication of the 2004 *Satellite Task Force Report*, there are many new satellite systems in various stages of development, deployment, and employment. As of September 2009, there are three packet processing regenerative Ka band satellites currently located in the GEO orbit over the United States. One commercial satellite has a raw capacity of 10 gigabits per second (Gbps) with about 100 uplink beams and 700 downlink beams, and is currently providing commercial IP packet services for enterprises, the Government, and consumers. A development program is integrating a packet-processing hosted payload (IP router in the satellite) on a commercial satellite for a near-term launch. Some commercial providers have recently announced their intentions to build very high capacity Ka band spot beam satellites with 100 Gbps capacity, now possible with the use of several uplink and downlink beams and spectrally efficient coding and modulation techniques. Such large capacity satellites could easily scale to support 20 to 30 megabits-per-second terminal speeds and thus allow COMSATCOM to directly compete with the wired terrestrial networking solutions.

[63] A mechanism to leverage a small, initial effort into something larger and more significant; similar to loading a computer program using a much smaller, initial program such as an operating system.

3.4.5 Technology Demonstrations—Space Based Network Nodes

The DoD is currently exploring the benefits of placing IP routers aboard commercial satellites. Under the DoD Joint Capabilities Technology Demonstration program, one organization has developed and will demonstrate a radiation-tolerant router to implement network services directly onboard a commercial communications satellite in 2010. Such space-based network nodes (SBNN) may offer several benefits as they are developed and deployed commercially.

Security Benefits

SBNNs provide benefits to the security of the RF, ground, and cyber segments and can be managed securely out-of-band from the SOC by a control bus that is separate from the main satellite bus. SBNNs may include an onboard route processing engine and an RF hub modem waveform, helping to mitigate RF spoofing and theft of service. SBNNs employ onboard processing, which reduces the ability to geolocate a transmitting terminal. SBNNs may also allow for the introduction of advanced features or new RF waveforms through use of an upgradeable software-based modem. Ground security benefits include a reduction in the reliance on teleports, as traffic does not have to be double-hopped to the teleport. User traffic can pass directly between satellite users on different transponders or spot beams, even in the event that the teleport is inactive or compromised. The value of SBNNs increases as more SBNNS are deployed across multiple satellites, because inter-satellite links can provide additional network resiliency in the event ground infrastructure is compromised. SBNNs may leverage existing cybersecurity features and network attack protections if they are evolved from terrestrial antecedents. SBNNs are part of a layered security architecture as an SBNN may be a potential target of a security threat similar to those of terrestrial network nodes.

Performance Benefits

SBNNs can reduce latency for satellite users since network traffic can be routed dynamically onboard a satellite, including across transponders and beam types, without having to double-hop to a teleport station. This reduction in latency can be significant for many real-time applications as the round-trip time delay between a geostationary satellite and a teleport can be up to 0.25 seconds. As part of a layered security architecture, SBNNs may be a potential target of a security threat similar to those of terrestrial network nodes.

Cost Benefits

A reduction in transponder and ground segment costs may be achieved with SBNNs as compared to bent-pipe solutions (which include more than one hop), because the reduced reliance on teleports for terminal-to-terminal communications means that fewer transponders are required.

Space Based Network Nodes Summary

SBNNs deployed onboard a satellite may dynamically route traffic between different satellite users without having to double-hop to the teleport, even if the users are on different transponders. The ability to avoid the double-hop to the teleport can increase security since the satellite can continue to function even if the ground teleport system is unavailable or compromised. SBNNs are regenerative, using onboard processing and decoupling the RF uplink and downlink, which can increase the security and performance of RF systems. SBNNs can be designed to leverage existing terrestrial network technologies, which increases cybersecurity by mitigating cyber attacks, and may integrate independent research and development from commercial technology leaders to reduce the cost to provide NS/EP network communications over a satellite.

4.0 CONCLUSIONS

The conclusions contained in this section are derived from the sections above and are in direct support of Section 5.0, Recommendations, below.

Interference
Interference presents a significant and growing operational risk to commercial satellite networks and their users, including those with NS/EP missions. It is commercially infeasible for industry to build systems that are immune to interference; however, direct Government financial support could be used to enhance commercial systems for Government use. While international mechanisms exist to address PI, most interference cases result from user error, equipment failure, or poor operational practices. Commercial operators noted that much of the interference currently experienced by Government users on commercial satellites is "self-inflicted" as a result of insufficient training of Government satellite terminal users. Additional training of Government users would reduce incidence of operator error.

Today, industry and Government do not jointly address interference issues as a systemic risk. Instead, Government becomes involved only when a specific Government service is affected. This narrow focus prevents Government and industry from developing the beneficial, broad situational awareness that would lead to earlier detection and resolution of suspected PI cases. Nascent technical approaches such as geolocation rely on information sharing processes that have yet to mature, particularly between Government and industry. The Government has not yet embraced industry efforts to share information and develop technical solutions, including improved training, embedded signal identification (carrier ID), and sharing of ephemerides and reference emitter data.

Cybersecurity
Today's large, global satellite operators maintain complex hybrid networks composed of both terrestrial and space assets. The terrestrial components of a satellite network contain many of the same subsystems—switching, routing, addressing, and authentication nodes—that are found in other communications networks. Like their terrestrial counterparts, these subsystems are vulnerable to malicious and inadvertent disruption. Thus, the mitigation techniques required to secure networks using communications satellites are essentially the same as those required to secure any other network.

With today's technology, the space component of a satellite network offers few obvious vulnerabilities. Most current satellites act as a passive repeater of the RF signal that is sent from Earth. As a result, there is little opportunity for malicious information to interact with the satellite system itself. Technologies that involve onboard processing provide additional benefits to satellite users, but may open up new satellite vulnerabilities.

The satellite control component does raise two risks that must be mitigated: (1) the potential for an adversary to remotely introduce a false satellite command; and (2) the potential for an adversary to prevent the satellite operator from transmitting commands or receive telemetry from the satellite. Today, satellite operators take extraordinary measures to prevent either of these occurrences.

Better information sharing and cyber response mechanisms are needed to adequately address the cyber threat to critical infrastructure and key resource sectors. Given the threat environment, and the global reliance on cyber technologies and networks, a national capability to prevent, detect, mitigate, and respond to cyber incidents of national consequence is critical to national security.

Avoiding Collisions in Space

Due to their location in space, satellites and their payloads are less likely than terrestrial facilities to be successfully targeted by physical attack. However, because in most cases satellites cannot be repaired once placed in space, catastrophic physical damage in orbit is usually permanent.

The near-Earth space environment contains orbital debris moving at a high velocity relative to satellites. Debris frequently transits the orbits of hundreds of operational manned and unmanned spacecraft and poses risks to current and future space systems. While accidental collisions between debris and an active satellite are unlikely, collisions do occur. In February 2009, an Iridium communications satellite collided with a defunct Cosmos satellite and generated 1,275 new pieces of trackable debris with enough kinetic energy to damage or destroy another spacecraft.

Every collision increases the amount of hazardous debris in the space environment. If left unchecked, this could pose a serious threat to the long-term viability of the space environment for operations, including human spaceflight. Objects colliding in satellite orbits experience very little atmospheric drag and can therefore remain in orbit for hundreds of years or more, posing continual risks to other satellites and generating additional debris. Accordingly, avoiding collisions and the resultant creation of additional space debris are of paramount importance. Collisions between controlled space objects can be avoided provided that operators communicate current satellite locations and plans for maneuvering their satellites. With sufficient space situational awareness, satellite operators can maneuver their craft away from uncontrolled space objects.

DoD uses its SSN to detect, track, catalog, and identify more than 19,000 man-made objects orbiting Earth. Today, DoD provides industry only limited access to its best space situational awareness information and lacks an automated process to incorporate the most accurate operator-supplied data on their commercial satellite locations and planned maneuvers into the DoD database; only lower-quality TLE data is made publicly available. Recently, leading satellite operators have started to explore the concept of pooling and standardizing their information exchange through an industry data center. Such a center would allow operators to augment existing TLE data with precise orbit data and maneuver plans from the operator's fleets and to develop common operational protocols for handling routine and emergency situations.

The Government can help assure the preservation of the space environment by establishing processes and standards to improve data collection, processing, collaboration, and timely sharing of the best space situational awareness data available with space users (including industry and international partners). The Government should also work with industry to explore ways to augment existing Government capabilities (such as data centers and sensor packages on commercial spacecraft).

Measures and Investments for Terrestrial Infrastructure

Today, major satellite network operators use redundant geographically diverse facilities for critical functions; it is unlikely that a single event would simultaneously impact both a primary and back-up Earth station. Most commercial providers maintain the back-up facilities and resources to respond to an attack or natural event. Satellite operators have independently established personnel security procedures, including background checks and pre-employment screenings, employee badges, logged entry and exit, and on-site security guards, as part of their best practices.

Operators' NOC, SOC, and TT&C sites are connected by multiple and cryptographically secure communications links that provide redundancy and path diversity. Additionally, ground stations utilize prevention and recovery techniques to mitigate risk. Preventative measures include creating buffer zones; use of multiple, diverse paths; using redundant circuits between sites; and robust security systems to protect NOC, SOC, and TT&C sites from attack.

Command Encryption on Commercial Satellites

Task force participants representing satellite owners noted that following the establishment of Government policy requiring satellite command uplink encryption, new satellites expected to be used for U.S. Government services are routinely equipped with NSA-approved cryptographic command receivers. As legacy in-orbit satellites without command encryption systems reach their end of life and are replaced, a growing portion of on-orbit satellite systems will support NSA-approved encrypted command operations.

Mission Assurance Working Group

Since its initiation in 2006, the MAWG has undertaken and addressed a variety of issues, including working to enhance compliance of COMSATCOM services with DoD mission assurance, protection, operations security, and network operations requirements. The MAWG continues to coordinate with providers to increase mission assurance through modifications and improvements to communications architectures, operational concepts for the employment and protection of COMSATCOM capabilities, and suggested new or revised capabilities for COMSATCOM service acquisitions.

In an effort to promote information sharing, the MAWG exchanges sensitive U.S. Government security-related information with cleared industry personnel whose systems (including U.S., foreign, and consortium systems) support national security and military forces, and to integrate industry participants into Government exercises and wargames that involve COMSATCOM issues. The MAWG has also examined policies, strategies, and operational concepts that provide assured access to sufficient levels of commercial bandwidth without interference to support national security, homeland security, and other peaceful purposes.

Lack of Long-Term Requirements Planning

The Government does not provide satellite carriers with a long-term forecast for DoD and other Government agencies' requirements. Typically, funding for DoD commercial SATCOM mobile and fixed satellite services comes from one-year increments of supplemental funding, as opposed to programmed funding lines, complicating efforts to make long-term forecasts. Without such information, satellite capacity may not be available at the proper time and place to meet Government needs for which carriers have not been given advance notice. Satellite operators continuously evaluate the possibilities to make investments in expansion capacity at new orbital locations/frequencies based on commercial opportunities as they arise, as well as routine planning for replacement of existing satellites with updated or enhanced systems. Since the design philosophy is to build highly efficient satellites that are customized for their orbital locations and thus cannot be readily redeployed to different orbital locations, planning cycles for replacement systems generally starts five years before the end of the 12-year nominal design lifetime of an existing system. In efforts to identify a strategy for establishing COMSATCOM as an enduring element of the overall global information grid (GIG), the DoD has directed a series of studies to examine future COMSATCOM bandwidth requirements and to assess the DoD COMSATCOM acquisition strategy. Results of these studies should be shared and discussed with industry to identify any opportunities for long-term planning related to the future role of COMSATCOM.

Commercial Satellite Industry Innovation

Commercial satellite systems are being enhanced with increased capacity and QoS to better support commercial and Government needs, including national communications systems and NS/EP. Recent deployments of systems with multiple narrow spot beams naturally reduce the effects of harmful RFI and add significantly more capacity. Advanced satellites with onboard processing provide improved connectivity, and reduce end-user reliance on centralized Earth stations; benefits include reduced latency, reduced cost, and more efficient use of terrestrial infrastructure. Additional innovations include systemic threat analysis during design time and implementation of security measures such as hardware-based identity for more robust cybersecurity.

Space Weapons

Due to the geopolitical nature of the satellite industry, the strategic situations in which satellites may be employed, and the availability and/or cost of mitigation capabilities, the commercial satellite industry acknowledges the risk of certain threats but does not attempt to mitigate them (for example, the effects of nuclear detonations, space weapons, and resilience of ground systems to chemical, biological, and radiological hazards). Since the industry can not afford to mitigate these threats, the Government should evaluate whether it should fund mitigation of these threats for critical COMSATCOM satellites and ground facilities used to support NS/EP communications.

5.0 RECOMMENDATIONS

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:

- **Direct the Secretary of Homeland Security to establish, consistent with the conclusion of the NSTAC *Cybersecurity Collaboration Report*, an operational mechanism for the Government and private sector to collaborate and coordinate to prevent, detect, mitigate, and respond, in a trusted environment, to cyber threats and cyber events**.
  - –Establish a Government-sponsored Joint Coordinating Center (JCC) for satellite industry representatives and other critical infrastructure and key resources sector stakeholders. The JCC's primary mission would focus on robust information sharing to develop and share cyber situational awareness, and would institutionalize the time-sensitive processes and procedures to detect, prevent, mitigate, and respond to cyber incidents of national and international consequence.
  - –The JCC would build upon the current capabilities of the National Coordinating Center for Telecommunications and the U.S. Computer Emergency Readiness Team, and incorporate other existing cyber incident monitoring and response entities.
  - –The JCC capability should be located in a Government facility with continuous operations, supporting tools, and collaboration capabilities.

- **Direct the Secretary of Defense and Secretary of Homeland Security to fund a comprehensive information sharing and operational collaboration program with key industry partners to systematically reduce electromagnetic and radio frequency interference**.
  - –The Government should establish a single joint industry-Government collaboration center to address planning and operational EMI/RFI issues.
  - –Early efforts between the DoD's Global SATCOM Support Center and industry, though focused on DoD, indicate that better integration between Government and industry on planning and operational matters would yield substantial benefits and help mitigate significant EMI/RFI vulnerabilities; the GSSC is one candidate to become the single Government focal point.
  - –DoD continues to develop and field systems to detect, identify, geolocate, and report on satellite service interference from both unintentional and deliberate sources. The level of proposed operational interaction and information sharing between DoD systems and the commercial satellite industry remains unclear, but such systems could become useful tools to help support commercial operator efforts to address interference.

- **Direct the Secretary of Defense to make safety of flight and the preservation of the space environment the leading national security drivers for enhanced space situational awareness efforts**.

  – The U.S. Government has a strong interest in preserving the space environment. Through improved data collection and processing, and close collaboration with industry, the Government can play an important role in encouraging safe and responsible space flight operations and can avoid the creation of unnecessary, dangerous space debris. In particular, DoD should:

  o Continue and expand the Commercial and Foreign Entities Program under which the U.S. Government currently shares orbital information with the private sector. In particular, the Secretary of Defense should provide high-accuracy Government data on existing space debris to all space operators and routinely share operational and flight data with commercial service providers. The data exchange between the U.S. Government and commercial operators should be automated to the greatest extent possible, and should include the most accurate, operator-supplied data on satellite locations and planned maneuvers. DoD, in conjunction with commercial operators, should begin to develop common operational protocols for handling routine and emergency situations.

  o Augment existing space surveillance capabilities through innovative programs such as hosting Government payloads/sensors on commercial satellites. Every satellite launched into space is potentially a sensor that can help extend the capabilities of an evolved Space Surveillance Network.

  o In conjunction with the Secretary of State, begin an international dialogue with other nations on space data sharing with the goal of merging national space catalogs and sensor data to create a more complete view of the space environment.

- **Direct the Secretary of Defense and the Secretary of Homeland Security to plan, in consultation with industry, for future satellite services, and to establish and enforce a uniform set of U.S. Government-wide mission assurance requirements (similar to that of the current DoD DSTS-G model) for fixed and mobile satellite communication providers serving the NS/EP community.**

  – Satellite operators routinely plan to replace existing satellites with updated or enhanced systems to meet commercial and potential Government user requirements. Unlike other commercial satellite users, the Government does not engage with industry in planning its long-term communication needs. Typically, funding for DoD commercial SATCOM mobile and fixed satellite services comes from one-year increments of supplemental funding, as opposed to programmed funding lines, making long-term forecasting difficult. As a result, the Government relies entirely on the "spot market" to meet long-term service needs, risking shortfalls in commercial satellite availability when critical needs arise. Representatives from the Government should meet with the commercial satellite industry no less than annually to engage in planning long-term communications needs.

- Some satellite operators have made substantial investments in new systems and procedures to meet evolving mission assurance requirements. The Government should build on the experience it has gained in the implementation of the information assurance process in the current DSTS-G contract to uniformly enforce its information security requirements for all of the satellite contracts that it awards. New processes should be implemented in a manner that provides an incentive for commercial providers to maintain and upgrade the security and integrity of networks used for critical NS/EP functions.
- The Government should make appropriate investments to ensure the availability of satellite-based priority communication services necessary to increase the robustness and reach of NS/EP Government communications, both before and during an emergency.
- Fund research and development to evolve key satellite solutions such as multiple spot beams and unified packet processing systems to enable next generation networks for integrated voice, video, and data services.

APPENDIX A:

PARTICIPANT LIST
TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER WORKING GROUP PARTICIPANTS

APPENDIX A: PARTICIPANT LIST

NSTAC MEMBERS, GOVERNMENT PERSONNEL, AND OTHER WORKING GROUP PARTICIPANTS

MEMBER COMPANY PARTICIPANTS

The Boeing Company	Mr. Marc Johansen, Chair
Intelsat General Corporation	Mr. Richard DalBello, Chair
Harris Corporation	Mr. Duane Selby
Lockheed Martin Corporation	Dr. Allen Dayton
Qwest Communications International, Incorporated	Ms. Kathryn Condello
Raytheon Company	Mr. Stephen Haynes
Rockwell Collins Incorporated	Ms. Leslie Blaker
Science Applications International Corporation	Mr. Hank Kluepfel
Teledesic Corporation	Mr. Doug Carter
Verizon Communications Incorporated	Mr. Marcus Sachs

OTHER WORKING GROUP PARTICIPANTS

Aerospace Corporation	Mr. Eric Aufderhaar
	Mr. Jack Clarke
The Boeing Company	Mr. William Reiner
	Mr. Robert Steele
Comtech EF Data	Mr. Robert Turner
Cisco Systems Incorporated	Mr. Duane DeCapite
	Ms. Julie Ann Connary
	Mr. Adam Golodner
Deloitte & Touche LLP	Mr. William O'Brien
DRS Technologies Incorporated	Mr. David Fields
	Mr. Dave Shields
Eutelsat SA	Mr. Joe Long
Harris Corporation	Mr. Richard White
Hughes Network Systems, LLC	Dr. Rajeev Gopal
Inmarsat, PLC	Mr. J.J. Shaw
Integral Systems	Ms. Joan Grewe
Intelsat General Corporation	Mr. Vinit Duggal
	Mr. Britt Lewis
	Mr. Sterling Winn
L3 Communications Corporation	Dr. Michael Frankel
LinQuest Corporation	Mr. Richard Gobbi

MITRE Corporation	Mr. Ed Hosken
	Mr. Mike Staso
Northrop Grumman Corporation	Mr. Peter Hadinger
Orbital Sciences Corporation	Mr. Ken Bell
Raytheon Company	Mr. Alan Goldey
	Mr. Frank Newell
Satellite Industry Association	Ms. Patricia Cooper
Science Applications International Corporation	Mr. William Chapman
	Mr. Steven Lines
SES S.A.	Mr. Timothy Deaver
	Mr. Robert Demers
	Mr. Andrew D’Uva
Telesat Holdings Incorporated	Mr. Martin Speckhardt
TerreStar Corporation	Mr. Stephen Carne
	Mr. Clive King
	Mr. Jeff Stern

U.S. GOVERNMENT PERSONNEL

Air Force Cyberspace Technical Center of Excellence	Lt. Col. Jeffrey Humphries
	Capt. Mark Hanus
Defense Information Systems Agency	Mr. Chris Gedo
	COL Allen Green
	Mr. William Janowsky (contractor)
	Mr. Jeffrey Prevett (contractor)
Department of Defense	Mr. James Mackin (contractor)
Department of Homeland Security	Mr. Dale Barr
	Dr. Edward Jacques (contractor)
	Mr. Rick Lichtenfels
	Mr. Gabriel Martinez
	Mr. Sean McGurk
	Mr. Will Williams
Federal Communications Commission	Mr. Shanti Gupta
National Space Security Office	Lt. Col. Jeffrey Kaczmarczyk

SATELLITE TASK FORCE BRIEFERS

The Boeing Company	Mr. Robert Vaughan
Cisco Systems Incorporated	Mr. Duane DeCapite
Defense Information Systems Agency	Mr. Chris Gedo
Fox Entertainment Group	Mr. Andy Setos
Hughes Network Systems	Dr. Rajeev Gopal
iDirect Incorporated	Mr. Dave Bettinger

Inmarsat PLC	Mr. Martyn Lewis
Intelsat General Corporation	Mr. Vinit Duggal
	Mr. Britt Lewis
Juniper Networks Incorporated	Mr. Robert Dix
MITRE Corporation	Mr. John Woodward
SES Engineering	Mr. Stewart Sanders

APPENDIX B:

ACRONYMS

APPENDIX B: ACRONYMS

AFSPC	U.S. Air Force Space Command
ASAT	Anti-Satellite
ASD/NII	Assistant Secretary of Defense for Networks & Information Integration
CFE	Commercial and Foreign Entities
CLIN	Contract Line Item Number
cm	Centimeters
CNSSP	Committee on National Security Systems Policy
COMSATCOM	Commercial Satellite Communications
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf
CNSS	Committee on National Security Systems
CSM	Communications Status Monitoring
DHS	Department of Homeland Security
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDI	Department of Defense Instruction
DSTS-G	Defense Information System Network (DISN) Satellite Transmission Service-Global
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
FCC	Federal Communications Commission
FCSA	Future COMSATCOM Services Acquisition
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FY	Fiscal Year
Gbps	Gigabits per Second
GEO	Geosynchronous Earth Orbit
GETS	Government Emergency Telecommunications Service
GIG	Global Information Grid
GSA	General Services Administration
GSSC	Global SATCOM Support Center
HAIPE	High Assurance Internet Protocol Encryptor
IA	Information Assurance
IADC	Inter-Agency Space Debris Coordination Committee
ID	Identification

IP	Internet Protocol
IPS	Intrusion Prevention System
JCC	Joint Coordinating Center
JSpOC	Joint Space Operations Center
km	Kilometers
LEO	Low Earth Orbit
MAC	Mission Assurance Category
MAWG	Mission Assurance Working Group
MILSTAR	Military Strategic and Tactical Relay [satellite]
NCS	National Communications System
NIST SP	National Institute of Standards and Technology Special Publication
NOC	Network Operations Centers
NSA	National Security Agency
NS/EP	National Security and Emergency Preparedness
NSSO	National Security Space Office
NSTAC	National Security Telecommunications Advisory Committee
NSTISSP	National Security Telecommunications and Information Systems Security Policy
PI	Purposeful Interference
PIRT	Purposeful Interference Response Team
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAIDRS	Rapid Attack Identification Detection Reporting System
RF	Radio Frequency
RFI	Radio Frequency Interference
SATCOM	Satellite Communications
SBNN	Space Based Network Node
SDA	Space Data Association
SIA	Satellite Industry Association
SME	Subject Matter Expert
SOC	Satellite Operations Centers
SRAS	Special Routing Arrangement Service
SSN	Space Surveillance Network
SP	Special Perturbation
STF	Satellite Task Force
TLE	Two-Line Element

TRANSEC	Transmission Security
TT&C	Telemetry, Tracking, and Command
USSTRATCOM	U.S. Strategic Command
WPS	Wireless Priority Service

APPENDIX C

PHYSICAL SECURITY QUESTIONNAIRE

APPENDIX C: PHYSICAL SECURITY QUESTIONNAIRE

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC)
CORE ASSURANCE TASK FORCE SURVEY
SATELLITE INDUSTRY

Background:

Executive Office of the President Goal: Examine the physical security of the major hubs/interconnections points for carriers/Internet service providers such as peering points, telecom hotels, satellite facilities, and cable landings. The purpose of this investigation is to determine what, if any, mitigation measures should be taken by the Government to assure physical security of the core network or key functions.

The NSTAC Core Assurance Study Group will build-on the existing body of knowledge and use this information to re-educate Government stakeholders, and determine if there is additional work to be done to contribute to the topic area. The task will be done by reviewing previous NSTAC reports and work from other groups related to physical security of networks. The products produced by this group will not address Internet security issues such as spam, viruses, malware, worms, Trojans, distributed denial of service attacks, and phishing. The focus of the group will be infrastructure threats and issues concerning the physical security of the core. The group will identify any existing deficiencies with physical core security and provide recommendations for Government action.

Survey Procedure: The Satellite Industry Association will circulate to members and key industry providers the following survey questions regarding the Physical Security aspects of the Core Network Elements and request responses for Satellite Based Facilities with respect to the threats listed above. **Responses will be kept confidential and should be provided to SIA by COB Thursday, October 1, 2008**.

The primary Core Network Elements are: (1) Satellite Ground Stations; (2) Teleports; (3) TT&C Facilities; (4) Network Operations Centers; and (5) Satellite Operations Centers. Responses should include any other ground-based facilities that respondents consider to be Core Elements.

Responses should also provide comments on any Government support to protect or restore Core Network Elements, as well as any recommendations on what additional support Government could provide to improve the physical security of core elements.

Threats To Be Considered:
All types of threats are considered against the operation of the core elements with the exception of the cyber related threats.

Natural Disaster threats include:

- Floods
- Tornadoes
- Hurricanes
- Thunderstorms and Lightening
- Winter Storms and Extreme Cold
- Extreme Heat
- Earthquakes
- Volcanoes
- Landslides and Debris Flow
- Tsunamis
- Fires
- Wildfires

Manmade Attacks

- Unintentional – Accidents
- Terrorist Attack Methods (refer to: DHS/Federal Bureau of Investigation Joint Special Assessment "Potential Terrorist Attack Methods" (FOUO), 23 April 2008
  - Aircraft as a Weapon
  - Biological Attack
  - Chemical Attack
  - Hostage Taking
  - Improvised Explosive Device
  - Maritime Vessel as a Weapon
  - Nuclear Attack
  - Radiological Dispersal Device
  - Guided Standoff Weapons
  - Unguided Standoff Weapons
  - Vehicle-Borne Improvised Explosive Device

SATELLITE INDUSTRY QUESTIONNAIRE

Survey Questions:

1) How are your Satellite Ground Stations, Teleports, NOCs, SOCs, and TT&C sites protected against each of the physical threats listed above?
2) Describe protection measures in place (e.g., facility lighting, fencing, security cameras, vehicle access to facility, chemical-biological-radiological protection, emergency power, high-altitude electromagnetic pulse protection, etc.). Note any recent improvements in protective measures (within the last 5 years).
3) Do you have a long range plan for addressing the physical security of your satellite ground assets? Identify "best practices" that are established to minimize the impacts of threats. Note any improvements planned for the future.
4) Does your company have:
   a) A back-up Network Operations Center?
   b) A back-up Satellite Operations Center?
   c) An alternate TT&C site for each satellite?
5) Does your need for physical protection measures change if it is public knowledge that your satellite system is hosting Government payloads?
6) How long can you operate each site without central electrical power, prior to refueling back-up generators?
7) What personnel security practices are in place, including background checks, employee badges, security guards?
8) What type of visitor control procedures does your company have in place?
9) Do you have plans that consider coordinated attacks against multiple core elements?
10) Identify any weaknesses and vulnerabilities in your Core Elements physical security and possible measures that might be used to improve security.
11) What are the threats that most concern you and what do you currently plan to mitigate?
12) Are your NOC, SOC, and TT&C sites connected by terrestrial communications links? What would be the impact on your NOC, SOC, and TT&C operations if there was a loss of connectivity on these links and what strategies are in place to mitigate such a loss?
13) What, if anything, is the Government (local, state, Federal) doing to support your efforts to detect physical threats to core network elements and to defend against them? To restore disruption of core network elements?
14) What, if anything, should the Government (local, state, Federal) be doing to support your efforts to detect physical threats to core network elements and to defend against them? To restore disruption of core network elements?

APPENDIX D

PHYSICAL SECURITY QUESTIONNAIRE RESULTS

APPENDIX D: PHYSICAL SECURITY QUESTIONNAIRE RESULTS

	CURRENT	WEAKNESSES / IMPACT	PLANNED / FUTURE
Protective Mechanisms for Ground Assets	• Access control systems (personnel and vehicle) / Electric gates / Master key systems • Closed Circuit Television (CCTV) / Security cameras • Grounding to prevent electric surges / Fire detection and suppression systems / De-icing procedures / compliance with seismic standards • Fencing / Walled facilities / Double-paned window glass with shatter resistant film / Outdoor lighting • Emergency / Redundant Power Source / Generators • Facilities located outside of populated areas, flood plains, or areas prone to tornadoes, hurricanes, landslides, debris flow, tsunamis, etc. constructed to survive natural elements. • Emergency evacuation plans in place / Conducting physical security surveys • Security Guards • Remote door alarm monitoring • Visitor registration procedures	• Non-standard access control and CCTV • Improve security guard and employee training to handle threats • Need to employ 24x7 or armed security guards • Facilities not designed to withstand nuclear detonation, electromagnetic pulse, or radiological fallout • Lack of redundant antenna compound or gateway equipment • Proximity of operations centers to public thoroughfares	• Conducting reviews and audits of security systems • Security cameras and remote monitoring • Increasing the presence of security guards and local law enforcement • Increase facility security to include badging, fencing, and uninterruptible power supply (UPS) protection • Document security baseline, single points of failure, and develop a survivability strategy • Maintain and implement Mission Assurance Category level compliance, OSHA (Occupational Safety and Health Administration) regulations, and Network Reliability & Interoperability Council (NRIC) best practices • Upgrade to a common control system • Avoid placing mated pairs in the same location, and avoid placing redundant logical facilities in the same path • Regularly test backup and secondary sites

	CURRENT	WEAKNESSES / IMPACT	PLANNED / FUTURE
Backup Mechanisms to Ensure Continuity of Operations	• Have Backup Network Operations Center: 55 percent • Have Backup Satellite Operations Center: 89 percent • Have alternate Telemetry, Tracking, & Command (TT&C) site for each satellite: 78 percent • NOC, SOC, and TT&C sites are connected by terrestrial data links: 100 percent	Minimal impact on NOC, SOC, and TT&C operations if there was a loss of connectivity on these links due to: • Interconnection with commercial satellite communications, physically diverse terrestrial communications links, diverse fiber rings, and diverse network sites • Short-term loss of communications while reconfiguring for satellite communications back-up • Have multiple landline paths and vendors • Direct link between SOC and NOC that does not require terrestrial communications links • Have satellite link in place in the event of a ground communications failure	• Ensure continuity of operations through backup facilities, generator power, geologically diverse facilities, having available hardware, or increasing the number of gateways
Physical Threats of Greatest Concern	• Manmade threats such as terrorism, cyber attacks • Natural threats such as floods, earthquakes • Access and visitor controls not universally applied and physical intrusion • Personnel safety • Network communications interruptions	DUE TO THE STRUCTURE OF THE QUESTIONNAIRE, NO QUESTION WAS ASKED THAT PROMPTED RESPONDENTS TO ANSWER THIS QUESTION	Mitigation measures for natural threats: • Prevention and restoration • Implementation of best practices and review of security measures • Encrypted virtual private network links • Transferring services to non-impacted area • Maintaining backup facility Access and visitor controls: • Creating and updated security policies • Creating a one-badge system • Networking all CCTV cameras Network Communications Interruptions: • Increase path diversity

	CURRENT	WEAKNESSES / IMPACT	PLANNED / FUTURE
Security Practices	Personnel Security Practices: • Employee badges • Pre-employment background screening • Security Guards • Logged entry and exit / Access control • Annual security training / Operations security awareness • CCTV / Security cameras / Remote monitoring • Grounds checks • Multi-factor authenticators • Personnel trained for emergency response • Visitor pre-screening and registration Visitor Control Practices • Sponsorship by an employee / Submit a request prior to the visit • Visitors escorted at all times • Visitor badge • Visitor entry / exit is logged • Proof of identity • Screening against Government databases • Searching bags and possessions	DUE TO THE STRUCTURE OF THE QUESTIONNAIRE, NO QUESTION WAS ASKED THAT PROMPTED RESPONDENTS TO ANSWER THIS QUESTION	DUE TO THE STRUCTURE OF THE QUESTIONNAIRE, NO QUESTION WAS ASKED THAT PROMPTED RESPONDENTS TO ANSWER THIS QUESTION
Government Support to Defend Against Physical Threats	• Reporting threats and providing intelligence and information sharing • Priority service for critical circuits and fuel delivery in the event of a crisis • Meteorological / Space Weather • Space situational awareness	• Protective measures for commercial providers will not change based on hosting a Government payload • Protective measures for commercial satellites would change based on Government requirements	• Funding for critical infrastructure upgrades • Make non-mandatory recommendations • Support slow growth initiatives around infrastructure complexes • Enforce and increase no fly zones • Limit information (satellite pictures) available on the Internet • Harden all sites against terrorist attacks

	CURRENT	WEAKNESSES / IMPACT	PLANNED / FUTURE
			• Identify dependant peer groups, programs, and/or treaties to activate emergency procedures if necessary • Share space situational awareness information and space weather data • Make Governments aware of facilities within their jurisdiction to respond in the event of an attack and to monitor facilities

* Numbered to reflect issue priority as determined by frequency of mentions in survey responses.

APPENDIX E

CYBERSECURITY QUESTIONNAIRE

APPENDIX E: CYBERSECURITY QUESTIONNAIRE

For all questions, please provide non-proprietary answers at a level of detail you believe is appropriate.

1) Would you be amenable to hosting Government payloads on your satellite systems to identify, alert, and/or protect against cyber, attack, jamming, and other threats?

- What factors would persuade or dissuade you from integrating such hosted payloads?

2) How do you believe Industry currently interacts with Government to secure and protect your satellites and networks from cyber attack, interference, or jamming?

- What is the Government's current involvement with your company?
- What do you believe the Government's role with Industry should be?
- What would you like the Government's role with your company to be?

3) Do your systems experience events that could be characterized as cyber attacks, interference, or jamming?

- How do you categorize and measure cyber events as actually rising to the level of "attacks"?
- If you differentiate between intentional and non-intentional events, do you see any trends?
- What is the nature of these events?
- Are any of these events unique to satellite services/architectures, or shared with other modes of communications technologies such as terrestrial wireless or wireline services?
- How frequently do the events occur?
- Are you able to attribute these events to locations and/or specific entities?

4) What kind of cyber protection/anti-jam negation measures do you currently implement (both in anticipation of and in response to events)?

- How could Government resources best be spent to assist you in anticipating and responding to these events?
- What level of Government resources would be required?
- How has your approach to anticipating, understanding, and mitigating these issues changed in the five (5) years since the NSTAC's 2004 satellite vulnerability study?

5) What organizational structures and/or formal cooperation mechanisms would facilitate better Government and Industry coordination on cyber threats, incidents, and responses?

- How regularly would Government-Industry interaction be required?
- Are there any specific initiatives you think would be beneficial?

6) What are your top three to five issues in the cyber area that require attention?

7) Do you have a person in your organization who is responsible for cybersecurity on an operational level?

8) How do you keep abreast of cybersecurity issues that may affect your network?

9) Please identify the satellite industry segment your organization represents:

- Satellite Services: ____
  - Mobile: ____ (Mobile Data: ____ Mobile Voice: ____)
  - Fixed: ____ (Broadband: ___ Private Networks: ___ Transponder Agreements: ___)
  - Remote Sensing: ____
  - Broadcasting: ____ (Satellite Television: ____ Satellite Radio: ____)
- Satellite Manufacturing: ____
  - Satellite Manufacturing: ____
  - Component and Subsystem Manufacturing: ____
- Launch Industry: ____
  - Launch Services: ____
  - Vehicle Manufacturing: ____
- Ground Equipment: ____
  - Network Equipment: ____ (Gateways: ___ Control Stations: ___ Very Small Aperture Terminals: ___)
  - Fixed: ____ (Direct Broadcast Satellite Dishes: ___ Handheld Satellite Phones: ___ Digital Audio Radio Service Equipment: ___ Global Positioning System Primary-Use Hardware: ___)

APPENDIX F

CYBERSECURITY QUESTIONNAIRE RESULTS

APPENDIX F: CYBERSECURITY QUESTIONNAIRE RESULTS

	CURRENT EXPERIENCE	AREAS FOR IMPROVEMENT	SUGGESTED MECHANISMS
Government-Industry Interaction	• Minimal security collaboration • Government seen primarily as customer and regulator • Ill-defined, cumbersome Government security standards and requirements • Industry interested in hosting Government payload with appropriate funding and feasibility	1. Greater information sharing** 2. Improved Government standards and requirements 3. Assistance with geolocation of interference 4. Education and awareness-raising initiatives for industry	• Working groups and similar forums to the Mission Assurance Working Group, NSTAC Satellite Task Force, and Satellite Industry Association • Government-industry meetings held quarterly/semi-annually or monthly • Regular Government reports or briefings on threats, incidents, and responses • Highlight industry best practices • *Other:* technology sharing, mechanisms to monitor traffic/network problems, alerts on known threats
Industry Experience with Cyber "Events"	• No consensus on understanding of "attack" • Frequent interference and jamming without significant security breach • Mixed ability to distinguish intentional from non-intentional events • Some limited geolocation ability	1. Geolocation assistance 2. Greater information sharing 3. Education and awareness 4. Technology investment and innovation 5. *Other:* vulnerability assessments, legal and regulatory issues, standardization	DUE TO THE STRUCTURE OF THE QUESTIONNAIRE, THIS QUESTION IS ANSWERED AND ACCOUNTED FOR THROUGHOUT THIS TABLE

	CURRENT EXPERIENCE	AREAS FOR IMPROVEMENT	SUGGESTED MECHANISMS
Industry Cybersecurity Defense Measures	• Reliant on encryption and general information technology best practices • Cybersecurity responsibility often assigned to Vice President-level professional in information technology/network security • Cyber awareness maintained by newsletters and trade publications, meetings/briefings, general Internet research, monitoring of internal network, and other mediums	1. Government-industry information sharing on threats 2. Geolocation assistance 3. Information and Government-Industry collaboration on meeting security requirements	• Updated and/or expanded directives and requirements • Government-run industry resources organization with dedicated funding • Government investment in common platforms for detecting and reporting cyber events • Government investment in geolocation technologies and communications fallback infrastructure • Enhanced penalties for cyber attacks

* Numbered to reflect issue priority as determined by frequency of mentions in survey responses.

APPENDIX G

GLOSSARY

APPENDIX G: GLOSSARY

Application Layer: The seventh layer of the Open Systems Interconnection (OSI) model. The point where the user application interfaces with the protocols to transfer data across the network.

Availability: Availability is the measure of the degree to which a system is operable and capable of initiating a mission at an unknown (random) time. Availability defines the percentage of time that a system or item of equipment is operational in accordance with a minimum set of prescribed operational or functional specifications or criteria. Space segment availability reflects the space segment's ability to meet the threshold set of communications requirements as a function of the connectivity key parameter.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Bandwidth: A measure of spectrum (frequency) use or capacity. For instance, a voice transmission by telephone requires a bandwidth of about 3000 cycles per second (3 KHz). A television channel occupies a bandwidth of 6 million cycles per second (6 MHz) in terrestrial Systems. In satellite-based systems a larger bandwidth of 17.5 to 72 MHz is used to spread or "dither" the television signal in order to prevent interference.

Bent Pipe: A description of a satellite communication architecture type in which data is transmitted to the satellite, which then sends it right back down again like a bent pipe. The only processing performed is retransmission of the signals.

Botnet: Computers that can be controlled by outside attackers that often gain control by inserting a virus, or other malicious software, into computers in an effort to provide an attacker access. Computers may be part of a botnet even if it operates normally. Botnets are often used to conduct a range of activities, from distributing spam and viruses to conducting denial of service attacks.

Communications Ground Station: Telecommunications network nodes communicate through satellites, typically with small antennas and low-cost electronics at user facilities, and large antennas with more complex data handling facilities at key traffic hubs. Hub Earth stations are generally owned by satellite operators or specialized satellite network providers.

Communications Security (COMSEC): Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Control Segment: Responsible for the operation of the overall satellite system, which includes platform control, payload control, and network control. The control segment consists of ground satellite control facilities, systems onboard the satellite and communications networks linking the control facilities.

Cybersecurity: No formal, accepted definition of cybersecurity currently exists; however, the International Telecommunication Union recently approved ITU-T X.1205 "Overview of Cybersecurity." This document states "cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability, integrity, which may include authenticity and non-repudiation, and confidentiality."

Cyberspace: *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* defines cyberspace as the interdependent network of information technology infrastructures, and include the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.[64]

Denial of Service: Any action or series of actions that prevents any part of an information system from functioning.

Downlink: The portion of a communications link used to transmit signals from a satellite to an Earth-based terminal (on land, ship, or aircraft).

Encryption: Encryption is the manipulation of packet data in order to prevent anyone but the intended recipient from reading it.

End-to-End: The inclusion of all requisite components necessary to deliver stated information exchange capability from the information producer's information appliance to the intended user information appliance(s). For SATCOM systems, this implies all components from the user access and display devices, sensors, all associated applications to include the various levels of networking and processing, and all related communications transport mechanisms and associated management services.

Gateway: Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. A ground station that acts as an interface between satellites in a system or a link between a satellite and entry into a terrestrial communications network. It is an interface point where dissimilar communications systems can be integrated together.

Global SATCOM Support Center: A DoD organization that provides support to joint forces with global operational SATCOM management, maintains situational awareness for current and

[64] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* May 2009.

future SATCOM operations, provides support to anomaly management and resolution, and acts as an interface with the DoD information operations infrastructure.

Hop: A communications signal that travels from the ground to the satellite and back to the ground. In some instances the signal needs to be sent to a second satellite, and then back down to the ground; this is called a double hop or two-hop operation.

Jamming: The deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability.

Link Layer: Layer 2 in the OSI reference model. Responsible for moving data in and out across a physical link.

Mission Assurance Category I (MAC I): Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.[65]

Mission Assurance Category II (MAC II): Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.[66]

Mission Assurance Category III (MAC III): Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.[67]

Network Layer: Layer 3 in the OSI reference model. Responsible for knowing the logical addresses of nodes, and for selecting routes through the network.

Network Operations Center (NOC): A location that monitors the operation of a network and usually provides efforts to solve connectivity and network problems. The NOC provides management of the terrestrial infrastructure by looking at configuration management and

[65] Department of Defense Instruction 8500.2, Information Assurance (IA) Implementation. February 2003.
[66] Ibid.
[67] Ibid.

lock-down status/network systems monitoring. Network systems monitoring control sits in the NOC on the terrestrial side and monitors traffic to and from the terrestrial NOC.

National Institute of Standards and Technology (NIST): Measurement standards laboratory that is a non-regulatory agency of the United States Department of Commerce. Promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

Open Systems Interconnection (OSI) Model: A standard reference model for communications between two hosts on a network.

Physical Layer: Layer 1 in the OSI reference model. Responsible for supporting the movement of bits on the physical medium.

Radio Frequency (RF): Any frequency within the electromagnetic spectrum normally associated with radio wave propagation. Organizations such as the Federal Communications Commission and International Telecommunication Union have divided the radio frequency spectrum into subdivisions for management purposes.

Route Hijacking: A routing-based denial of service attack involves attackers manipulating routing table entries to deny service to legitimate systems or networks.

Satellites: Craft positioned hundreds to thousands of miles in space to efficiently relay a wide variety of broadcast and two-way communications across great distances.

Satellite Communications (SATCOM): A satellite communications system is comprised of three segments: Space Segment, Control Segment, and Terminal (Ground) Segment.

Satellite Control Stations: Monitor satellite health and command the mission operations and maintenance functions of satellites and system components. Satellite control stations are typically divided into the SOC and the NOC.

Satellite Operations Center (SOC): One or more facilities that supports space segment operations by providing pre-launch planning, launch and early orbit support, and satellite control functions. SOC personnel perform satellite command and control during launch, on-orbit test, and deployment, and assist in major anomaly resolution.

Space Segment: There are two parts to the space segment: ground elements and satellite(s), each comprised of platform (the basic structure and subsystems of the satellite) and payload. The payload provides space-based capabilities to the users and distinguishes one type of satellite from another.

Terminal (Ground) Segment: This segment comprises the actual equipment that receives and transmits signals to the satellite. Terminals can vary from a hand-held or man-pack terminal to a large fixed installation.

Terrestrial Data Links: Network connections that tie together the control stations, ground stations, and the rest of the terrestrial telecommunications infrastructure.

Transmission Security (TRANSEC): Component of COMSEC resulting from the TRANSEC application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

Transport Layer: Layer 4 of the OSI reference model. Ensures the reliable delivery of messages and provides error-checking mechanisms.

Uplink: The portion of a communications link used to transmit signals from an Earth-based terminal (on land, ship, or aircraft) to a satellite.

Very Small Aperture Terminal (VSAT): Refers to small Earth station employing a satellite antenna with a diameter or cross-section dimension in the general range of 1.2 to 2.4 meters. VSAT terminals are used in networks that primarily support point-to-multipoint communications as part of large private networks, particularly in large retail networks to support transactions such as inventory management and credit-card authorizations.

Virus: A virus is a computer program that spreads by infecting files or portions of a computer or router's hard drive, and then copies itself. Viruses range in severity and spread through user action including opening email attachments or sharing media, such as USB drives.

Worms: Worms are a type of virus that consume memory and network bandwidth, and can ultimately cause a computer to stop responding. Worms can permit an attacker to access computers remotely and require no user action to spread.

APPENDIX H

EXECUTIVE ORDERS AND PRESIDENTIAL DIRECTIVES

APPENDIX H: EXECUTIVE ORDERS AND PRESIDENTIAL DIRECTIVES

Executive Order 12472 - Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 3, 1984

"The National Communications System (NCS) was established by Executive Order (EO) 12472 as a Federal interagency group assigned national security and emergency preparedness (NS/EP) telecommunications responsibilities throughout the full spectrum of emergencies. Under the policy objectives stated in EO 12472 and National Security Decision Directive (NSDD) 97, these responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve measurable improvements in survivability, interoperability, and operational effectiveness under all conditions and seeking greater effectiveness in managing and using national telecommunication resources to support the Government during any emergency."[68]

Executive Order 13407 - Public Alert and Warning System, June 26, 2006

"It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster, or other hazards to public safety and well-being (public alert and warning system), taking appropriate account of the functions, capabilities, and needs of the private sector and of all levels of government in our Federal system, and to ensure that under all conditions the President can communicate with the American people."[69]

Presidential Decision Directive/NSC-63 - Critical Infrastructure Protection, May 22, 1998

Presidential Decision Directive/NSC-63 discussed the essential critical infrastructures that maintain the minimum economic and Government operations including telecommunications, energy, banking and finance, transportation, water systems, and Government and private emergency services. Presidential Decision Directive/NSC-63 addressed critical infrastructure vulnerabilities from equipment failure, human error, weather and other natural causes, and physical and cyber attacks. HSPD-7 Subject: Critical Infrastructure Identification, Prioritization, and Protection, supersedes Presidential Decision Directive/NSC-63.

Homeland Security Presidential Directive / HSPD-7 - Subject: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003

"This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[70] HSPD-7 supersedes Presidential Decision Directive/NSC-63.

[68] U.S. General Services Administration, http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/Executive%20Orders.12472_R2-u-s4-k_0Z5RDZ-i34K-pR.doc

[69] The National Archives, Federal Register, Vol. 71, No. 124. http://edocket.access.gpo.gov/2006/pdf/06-5829.pdf

[70] http://www.whitehouse.gov/omb/memoranda/fy04/m-04-15.pdf

Homeland Security Presidential Directive / HSPD-8 – Subject: National Preparedness, December 17, 2003

"This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities."[71]

National Security Presidential Directive/NSPD-51 / Homeland Security Presidential Directive/HSPD-20 - Subject: National Continuity Policy, May 9, 2007

"This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes "National Essential Functions," prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency."[72] NSPD-51 / HSPD-20 supersedes Presidential Decision Directive 67 Enduring Constitutional Government and Continuity of Government Operations.

These are Federal programs that address communications during a disaster (of any source) and the plans to accommodate public safety/continuity of Government:

- SAFECOM http://www.safecomprogram.gov/SAFECOM/
- National Response Framework http://www.fema.gov/emergency/nrf/

[71] http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm
[72] http://georgewbush-whitehouse.archives.gov/news/releases/2007/05/20070509-12.html

APPENDIX I

REFERENCE LIST

APPENDIX I: REFERENCE LIST

An Assessment of the Risk to the Cybersecurity of the Public Network. NSTAC and Government Network Security Information Exchanges. August 2009.

Burrell, James. *Disruptive Effects of EMI on Communications and Electronic Systems*. April 2003.

Center for Space Standards and Innovation, *CeleTrak.com*.

Chandler, Captain Roy. *Total Force 'RAIDRS' keep high frontier secure*. Air Force Times Online, January 2008.

Committee on National Security Systems. *National Information Assurance (IA) Glossary*. CNSS Instruction No. 4009. Revised June 2006

Committee on National Security Policy Systems Policy No.12, Subject: *National Information Assurance Policy for Space Systems Used to Support National Security Missions*. March 2007.

Department of Defense Directive 8581.1, Subject: *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*. June 2005.

Department of Defense Instruction 8500.2, *Information Assurance (IA) Implementation*. February 2003.

Executive Office of the President. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. 2009.

Executive Order 12472 - Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 23, 1984.

Executive Order 13407 - Public Alert and Warning System, June 26, 2006.

Federal Communications Commission Second Report and Order 04-130 – Mitigation of Orbital Debris, Released June 21, 2004.

Federal Information Security Management Act of 2002. Public Law 107-347; Title III. December 17, 2002.

Homeland Security Presidential Directive / HSPD-7 - Subject: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.

Homeland Security Presidential Directive / HSPD-8 - Subject: National Preparedness, December 17, 2003.

National Aeronautics and Space Administration. *Orbital Debris Quarterly News,* Volume 11, Issue 2, April 2007.

National Aeronautics and Space Administration. *Orbital Debris Quarterly News*, Volume 13, Issue 1, January 2009.

National Aeronautics and Space Administration. *Orbital Debris Quarterly News*, Volume 13, Issue 3, July 2009.

National Institute of Standards and Technology Special Publication 800-53. *Recommended Security Controls for Federal Information Systems and Organizations*. August 2009.

National Security and Homeland Security Presidential Directive / NSPD 51 / Homeland Security Presidential Directive / HSPD 20; May 9, 2007.

NSTAC Cybersecurity Task Force. *Cybersecurity Collaboration Report*. May 2009.

NSTAC Core Assurance Task Force. *NSTAC Report to the President on Physical Assurance of the Core Network*. November 2008.

NSTAC Global Positioning System Task Force. *NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS)*. February 2008.

NSTAC Satellite Task Force. *Satellite Task Force Report*. March 2004.

National Aeronautics and Space Administration. Orbital Debris Quarterly News, Volume 11, Issue 2, April 2007.

Presidential Decision Directive/NSC-63 Critical Infrastructure Protection, May 22, 1998.

Satellite Industry Association. *State of the Satellite Industry Report*. June 2009.

Security Space Index. *Space Security 2008*. September 2008.

United States Strategic Command. *FY07 Commercial Satellite Communications (COMSATCOM) Usage report (FOUO)*. February 2009.