United States General Accounting Office

GAO

Report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate

August 2002

CRITICAL INFRASTRUCTURE PROTECTION

Commercial Satellite Security Should Be More Fully Addressed

G A O

Accountability ★ Integrity ★ Reliability

United States General Accounting Office

August 2002

GAO
Accountability★Integrity★Reliability

Highlights

CRITICAL INFRASTRUCTURE PROTECTION
Commercial Satellite Security Should Be More Fully Addressed

Highlights of GAO-02-781, a report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, United States Senate.

Why GAO Did This Study

Because the federal government relies on commercial satellites, security threats leading to their disruption or loss would put government functions (including communications and information transmission) at significant risk. Accordingly, GAO was asked to review, among other things, the techniques used by federal agencies to reduce the risk associated with using commercial satellite systems, as well as efforts to improve satellite system security undertaken as part of federal efforts in critical infrastructure protection.

What GAO Recommends

To ensure that these assets are protected from unauthorized access and disruption, GAO recommends that steps be taken to promote the appropriate development and implementation of policy regarding the security of satellite systems. GAO also recommends that commercial satellites be identified as a critical infrastructure (or as part of an already identified one) in the national critical infrastructure protection strategy.

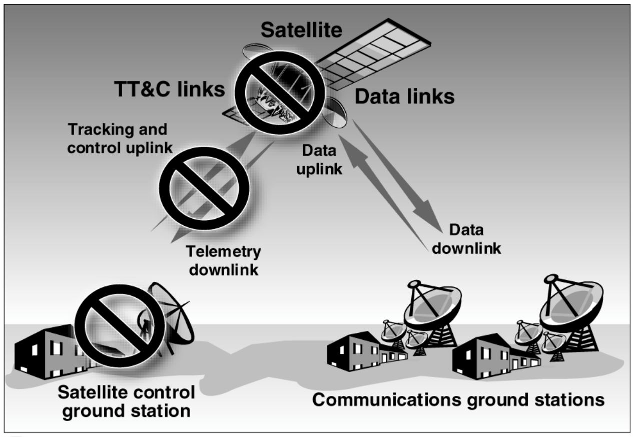
In commenting on a draft of this report, agencies included in our review concurred with our findings and recommendations. In addition, these agencies and private-sector entities provided technical comments, which were included in the report, as appropriate.

What GAO Found

Although federal agencies rely on commercial satellites, federal customers do not dominate the commercial satellite market, accounting for only about 10 percent of it. As a result, federal customers generally have not influenced security techniques used for commercial satellites. Federal agencies do reduce their risk by securing those system components under their control—the data links and communications ground stations—but most components are typically the responsibility of the satellite service provider: the satellite; the telemetry, tracking, and control links; and the satellite control ground stations (see figure below). Some federal agencies also mitigate risk by relying on redundant or backup capabilities, such as additional satellite services.

In 1998, Presidential Decision Directive 63 was issued to improve the federal approach to protecting our nation's critical infrastructures (such as telecommunications, energy, banking and finance, and transportation) by establishing partnerships between private-sector entities and the federal government. To date, the satellite industry has not been included as part of this national effort. Further, federal policy governing the security of satellite systems used by agencies addresses only those satellites used for national security information and pertains only to techniques associated with the links between ground stations and satellites or links between satellites. Without appropriate governmentwide policy to address the security of all satellite components and of non–national-security information, federal agencies may not, for information with similar sensitivity and criticality, consistently (1) secure data links and communication ground stations or (2) use satellites that have certain security controls that enhance availability.

Commercial Satellite System Showing Components Not Controlled by Government Agencies


Satellite
TT&C links
Data links
Tracking and control uplink
Data uplink
Telemetry downlink
Data downlink
Satellite control ground station
Communications ground stations

⊘ Satellite components not controlled by federal agencies

Source: GAO analysis.

This is a test for developing highlights for a GAO report. The full report, including GAO's objectives, scope, methodology, and analysis is available at www.gao.gov/cgi-bin/getrpt?GAO-02-781. For additional information about the report, contact Robert Dacey (202-512-3317). To provide comments on this test highlights, contact Keith Fultz (202-512-3200) or E-mail HighlightsTest@gao.gov.

Contents

Letter

Appendixes

Tables

Figures

Abbreviations

CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CIP	critical infrastructure protection
CNSS	Committee on National Security Systems
DOD	Department of Defense
EMP	electromagnetic pulse
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GPS	Global Positioning System
HHS	Department of Health and Human Services
ISAC	information sharing and analysis center
NASA	National Aeronautics and Space Administration
NCC	National Coordinating Center for Telecommunications
NDIA	National Defense Industrial Association
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTIA	National Telecommunications and Information Administration
NTISSP	National Telecommunications and Information Systems Security Policy
OSTP	Office of Science and Technology Policy
PDD	Presidential Decision Directive
RF	radio frequency
TT&C	tracking, telemetry, and control

G A O
Accountability ★ Integrity ★ Reliability

United States General Accounting Office
Washington, D.C. 20548

August 30, 2002

The Honorable Susan Collins
Ranking Minority Member
Permanent Subcommittee on Investigations
Committee on Governmental Affairs
United States Senate

Dear Senator Collins:

Government and private-sector entities rely on satellites for services such as communication, navigation, remote sensing, imaging, and weather and meteorological support. Although the government owns satellites, it also relies for certain services on satellites owned and operated by commercial satellite service providers. For example, the Department of Defense (DOD) typically relies on commercial satellites to fulfill its communications and information transmission requirements for non–mission-critical data and to augment its military satellite capabilities. The importance of commercial satellites for DOD is evident during times of conflict: according to a DOD study, commercial communications satellites were used in 45 percent of all communications between the United States and the Persian Gulf region during Desert Shield/Desert Storm.[1] Further, the federal government's reliance on commercial satellites is expected to grow.

The commercial satellite industry is also a critical component of the worldwide and national economy: the industry generated $85 billion in revenue in 2000. Accordingly, disruption of satellite services, whether intentional or not, can have a major adverse economic impact. One indication of the importance of satellite services was provided in 1998 by the failure of the Galaxy IV satellite, which disrupted 80 to 90 percent of 45 million pagers across the United States for 2 to 4 days and blocked credit card authorization at point-of-sale terminals (such as gasoline pumps).

Satellites are vulnerable to various threats. Protecting satellite systems against these threats requires attention to (1) the satellite; (2) the satellite control ground stations, which perform tracking and control functions to ensure that satellites remain in the proper orbits and which monitor satellite performance; (3) the communications ground stations, which

[1] National Air Intelligence Center, *Threats to U.S. Military Access to Space*, Document 1422-0989-98 (Wright Patterson Air Force Base, Ohio).

process the data being sent to and from satellites; and (4) communications links between satellites and ground stations—both those that transmit the tracking and control information and those that transmit the data. Security threats to any part of the system could put government and commercial functions at significant risk. Accordingly, at your request, we reviewed (1) what security techniques are available to protect satellite systems from unauthorized use, disruption, or damage; (2) how federal agencies reduce the risk associated with their use of commercial satellite systems; and (3) what federal critical infrastructure protection (CIP) efforts are being undertaken to address satellite system security through improved government and private-sector cooperation. To accomplish these objectives, we reviewed technical documents, policy, and directives and interviewed pertinent officials from federal agencies and the private sector involved in developing, operating, maintaining, and protecting satellite systems. Appendix I provides further details on our objectives, scope, and methodology.

Results in Brief

Techniques to protect satellite systems from unauthorized use and disruption include the use of robust hardware on satellites, physical security and logical access controls[2] at ground stations, and encryption of the signals for tracking and controlling the satellite and of the data being sent to and from satellites. Commercial satellite service providers stated that they provide some of these security techniques to meet most of their customers' security requirements and that they base their decisions on business objectives. For example, commercial satellite providers stated that they use backup satellites and redundant satellite features to ensure availability. However, commercial satellite providers generally do not use the more stringent techniques used in national security satellites for protection against deliberate disruption and exploitation.

When using commercial satellites, federal agencies reduce risks by securing the data links and ground stations that send and receive data. However, federal agencies do not control the security of the tracking and control links, satellites, or tracking and control ground stations, which are typically the responsibility of the satellite service provider. Further, although the federal government relies on commercial satellites, federal

[2] Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers (IDs), passwords, or other identifiers that are linked to predetermined access privileges.

customers make up only about 10 percent of the commercial satellite market and accordingly have had limited influence over security techniques employed by commercial satellite service providers. To mitigate risk, some federal agencies also rely on redundant or backup capabilities, such as additional satellite services. Aspects of satellite system security have been addressed in federal policy, but this policy is limited because it pertains only to satellite and supporting systems that are used for national security information, addresses only techniques associated with the links, and does not have an enforcement mechanism. Without appropriate governmentwide policy to address the security of all satellite components and of non–national-security information, federal agencies may not, for information with similar sensitivity and criticality, consistently (1) secure data links and communication ground stations or (2) use satellites that have certain security controls that enhance availability. Recent initiatives by the Executive Branch have acknowledged these policy limitations, but we are not aware of specific actions to address them.

It is important to our nation's economy and security to protect against attacks on its computer-dependent critical infrastructures (such as telecommunications, energy, and transportation), many of which are privately owned. In 1998, Presidential Decision Directive 63 was issued to improve the federal approach to protecting our nation's critical infrastructures by establishing partnerships between private-sector entities and the federal government. However, the satellite industry has not been included as part of this national effort, and there are no plans to include it. In addition, the July 2002 national strategy for homeland security does not suggest that the satellite industry be included in the approach to protecting our critical infrastructures.[3] In light of the nation's growing reliance on commercial satellites to meet military, civil, and private-sector requirements, omitting satellites from our nation's approach leaves a critical aspect of our nation's infrastructures without focused attention.

Because of the importance of the satellite industry to our nation, we recommend that steps be taken to promote appropriate revisions to existing policy and the development of new policy regarding the security of satellite systems, to ensure that federal agencies appropriately address the use of commercial satellites, including the sensitivity of information, security techniques, and enforcement mechanisms. In addition, we are

[3] Office of Homeland Security, *National Strategy for Homeland Security* (Washington, D.C.: July 2002).

recommending that commercial satellites be identified as a critical infrastructure sector (or as part of an already identified critical infrastructure sector) in the national CIP strategy, to help ensure that these assets are protected from unauthorized access and disruption.

We received written comments on a draft of this report from the Department of Defense; the National Oceanic and Atmospheric Administration, Department of Commerce; and the National Aeronautics and Space Administration. The Departments of Defense and Commerce and the National Aeronautics and Space Administration concurred with our findings and recommendations (see apps. II, III, and IV, respectively) and provided technical comments that have been incorporated in the report, as appropriate (some of these technical comments are reproduced in the appendixes). We received technical oral comments from officials from the Critical Infrastructure Assurance Office, Department of Commerce; Federal Aviation Administration, Department of Transportation; Office of Management and Budget; and United States Secret Service, Department of Treasury; in addition, we received written and oral technical comments from five participating private-sector entities. Comments from all these organizations have been incorporated into the report, as appropriate.

Background

Satellites provide many significant services, including communication, navigation, remote sensing, imaging, and weather and meteorological support. Satellites support direct radio communication and provide television broadcast and cable relay services, as well as home reception. Satellite services also support applications such as mobile and cellular communication, telemedicine, cargo tracking, point-of-sale transactions, and Internet access. Satellites also provide redundancy and backup capabilities to ground-based communications, as was demonstrated after the events of September 11, 2001, when satellites provided critical communications while ground-based lines were unavailable.

The commercial satellite industry includes manufacturers, the launch industry, service providers, and ground equipment manufacturers. Manufacturers design and build satellites, supporting systems, and ground stations. The launch industry uses launch vehicles, powered by rocket engines, to place satellites in orbit. Once commercial satellites are in orbit, they are operated by service providers, who lease available services. Commercial satellite service clients include telecommunication companies, television networks, financial institutions, major retailers, Internet service providers, and governments. Some companies resell leased satellite services to their clients. For example, major telecommunication companies sometimes include satellite services in their product line. Ground equipment manufacturers build and sell the items needed to use satellite services, such as ground station hardware (antennas), data terminals, mobile terminals (truck-mounted units), and consumer electronics (satellite phones). For the year 2000, the commercial satellite industry generated revenues of $85.1 billion:[4] $17.2 billion for satellite manufacturing, $8.5 billion for the launch industry,[5] $41.7 billion for satellite services, and $17.7 billion for ground equipment manufacturing,[6] according to an industry association.

Federal agencies also own and operate satellites. For example, the U.S. military and intelligence communities have satellites to provide capabilities for reconnaissance, surveillance, early warning of missile launches, weather forecasts, navigation, and communications. In addition, some federal civilian agencies own satellites that are used for communications, scientific studies, and weather forecasting.

Further, federal agencies use commercial satellites for services such as communications, data transmission, and remote sensing. For example, DOD typically relies on commercial satellites to fulfill its communications and information transmission requirements for non–mission-critical data and to augment its military satellite capabilities. The National Defense Industrial Association (NDIA) reported in December 1998 that the government's overall use of commercial satellites for communications and

[4] All revenues include payments made to subcontractors.

[5] The amount for launch services includes revenues from both government-owned and commercially owned payloads.

[6] The manufacturing indicators include amounts from commercial companies manufacturing for both government and commercial customers.

remote sensing is expected to grow significantly because of increased communications requirements. According to a DOD official, the department's reliance on commercial satellites is expected to grow through 2020. After 2020, DOD officials anticipate that commercial satellites will provide only surge capacity, as additional military satellites are expected to be operational. In addition to the U.S. military, several civilian government agencies also rely on commercial satellite systems. Table 1 provides brief descriptions of the use of commercial satellites by four civilian agencies included in our review.

Table 1: Civilian Agency Use of Commercial Satellites

Agency	Use of commercial satellites
National Aeronautics and Space Administration	To serve as an alternative means of transmitting launch commands and scientific data when there are geographical limitations to terrestrial communications networks
United States Secret Service	To provide, on a limited basis, communications when other methods are not available
Federal Aviation Administration	To transmit corrected Global Positioning System data to aircraft and for remote location air traffic control communications
National Oceanic and Atmospheric Administration/ National Weather Service	To disseminate imagery, graphic, and text data on weather conditions around the earth

Source: Cited agencies.

Collectively, the federal government does not dominate the commercial satellite market. According to commercial satellite industry officials, the revenue provided to the satellite industry by the federal government represents about 10 percent of the commercial satellite market.

However, the importance of commercial satellites for government operations is evident during times of conflict. For example, according to a DOD study, commercial communications satellites were used in 45 percent of all communications between the United States and the Persian Gulf region during Desert Shield/Desert Storm. Further, during operations in Somalia from December 1992 through March 1994, U.S. military and commercial satellite coverage was not available, so Russian commercial satellites were used. DOD currently reports approximately 50 percent reliance on commercial satellites for wideband services,[7] which are leased through the Defense Information Systems Agency's Commercial Satellite Communications Branch.[8]

The commercial satellite industry is a global industry that includes many foreign-owned corporations as well as partnerships between U.S. and foreign corporations. As a result, the U.S. government depends on foreign and international companies. For example, some commercial space systems of foreign origin are used by the U.S. military for imagery and communications support. NDIA reported that foreign ownership of satellites is expected to grow and predicted that by 2010, 80 percent of commercial communication satellite services could be provided by foreign-owned companies. This globalization of the satellite industry could affect the availability of commercial satellite systems to U.S. government or commercial entities through frequency allocations, tariffs, politics, and international law.

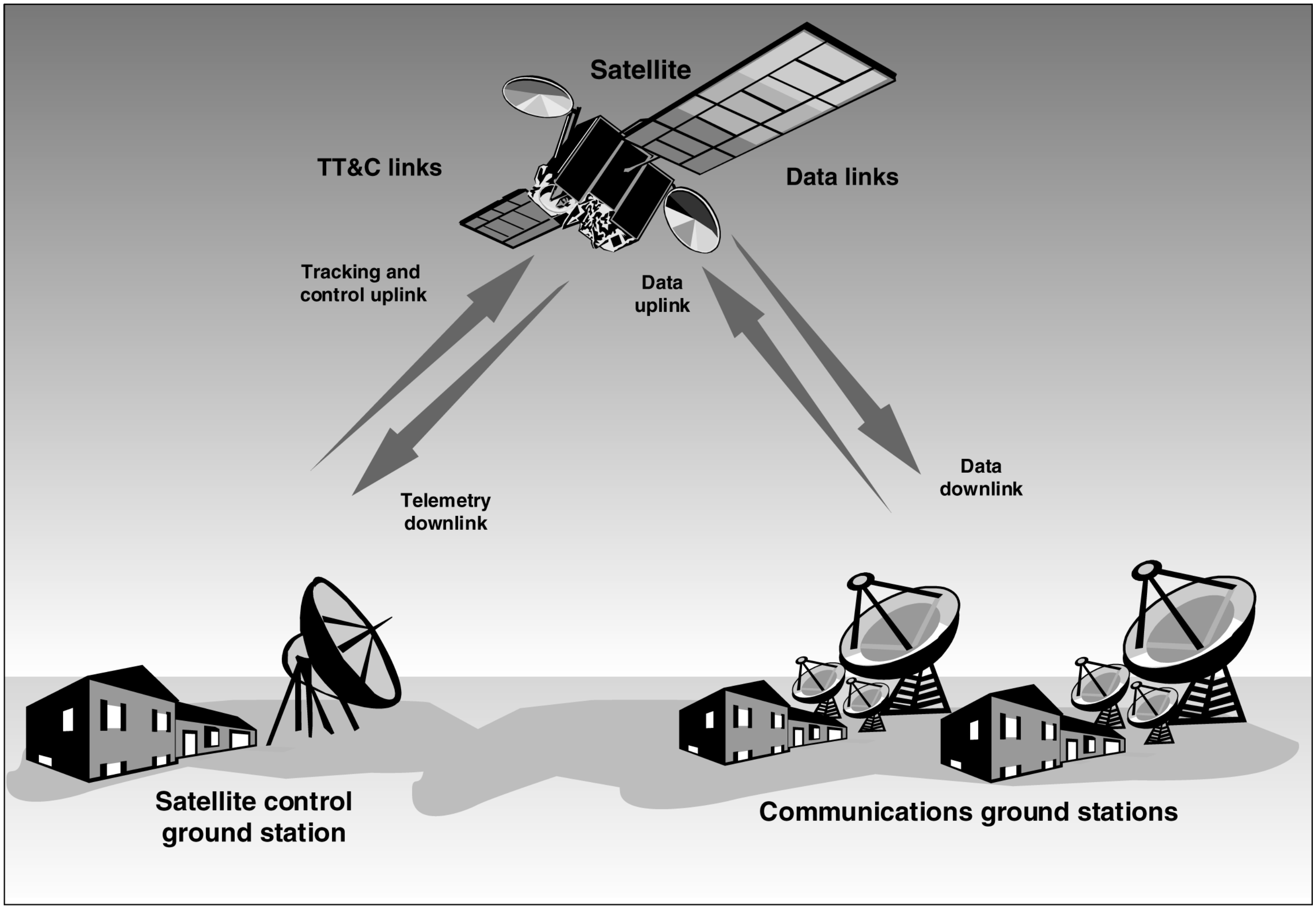
Satellites Operate through a System of Links and Ground Stations

A satellite system consists of ground stations, tracking and control links (commonly referred to as the tracking, telemetry, and control (TT&C) links) and data links, and satellites. Figure 1 illustrates the basic satellite system components.

[7] Wideband encompasses data rates greater than 64 kilobits per second.

[8] The Defense Information Systems Agency's Commercial Satellite Communications Branch is responsible for leasing commercial satellite services for DOD.

Figure 1: Key Components of a Satellite System


Satellite
TT&C links
Data links
Tracking and control uplink
Data uplink
Telemetry downlink
Data downlink
Satellite control ground station
Communications ground stations

Source: GAO analysis.

As the figure shows, two kinds of ground stations are associated with satellites: control stations and communications stations. Control stations perform tracking and control functions to ensure that satellites remain in the proper orbits (commonly referred to by the industry as “station keeping”) and to monitor their performance. Communications ground stations process imagery, voice, or other data and provide, in many cases, a link to ground-based terrestrial network interconnections.

The links between the two types of ground stations and the satellites are referred to by their function: TT&C and data links. TT&C links exchange commands and status information between control ground stations and satellites. Data links exchange communications, navigation, and imaging data between communications ground stations and satellites. As shown in figure 1, links are also distinguished by the direction of transmission: uplinks go from Earth to space, and downlinks from space to Earth. Satellites can also communicate with each other; these links are referred to as cross-links.

The final component of the system is the satellite. Every satellite has a "payload" and a "bus." The payload contains all the equipment a satellite needs to perform its function, and it differs for every type of satellite. For example, the payload for a weather satellite includes cameras to take pictures of cloud formations, while the payload for a communications satellite includes transponders to relay data (for example, television or telephone signals).[9] The bus carries the payload and additional equipment into space and provides electrical power, computers, and propulsion to the entire spacecraft. A satellite can serve simply as a relay between a source and a destination (for example, a communications satellite), or it can perform processing of data and communicate the data to a communications ground station (for example, an imaging satellite).

Satellite Systems Are Vulnerable to a Range of Threats

Satellite systems face unintentional threats to all parts of the system; such threats can be ground-based, space-based, and interference-oriented. The probability of these threats occurring and the difficulty of exploiting these vulnerabilities vary. Table 2 displays some of these threats and the vulnerable components.

[9] A transponder is an automatic device that receives, amplifies, and retransmits a signal on a different frequency.

Table 2: Unintentional Threats to Commercial Satellite Systems

Type of threat	Vulnerable satellite system components
Ground-based:	
Natural occurrences (including earthquakes and floods; adverse temperature environments) Power outages	Ground stations; TT&C and data links
Space-based:	
Space environment (solar, cosmic radiation; temperature variations) Space objects (including debris)	Satellites; TT&C and data links
Interference-oriented:	
Solar activity; atmospheric and solar disturbances Unintentional human interference (caused by terrestrial and space-based wireless systems)	Satellites; TT&C and data links

Source: DOD and GAO analysis.

Ground stations are vulnerable to damage or destruction by natural terrestrial threats such as earthquakes, floods, thunderstorms, lightning, dust storms, heavy snows, tropical storms, tornadoes, corrosive sea spray, and salt air. In addition, they could also be affected by natural conditions and environmental hazards, such as air pollution and adverse temperature environments, as well as power outages.

Satellites are physically vulnerable to space-based environmental anomalies resulting from natural conditions and man-made artifacts. Space-based threats include solar and cosmic radiation and related phenomena, solar disturbances, temperature variations, and natural objects (meteoroids and asteroids). In addition, the growing number of satellites is contributing to the problem of space “junk” (spacecraft and debris). As of May 2002, DOD identified over 9,000 man-made objects in space, including active satellites. As additional satellites are developed and deployed, DOD officials stated that the threat of collisions caused by the proliferation of satellites and accompanying debris could increase.

Links are vulnerable both to natural conditions (in space and in the atmosphere) and to congestion. Links can be severely degraded by the effects of solar activity and atmospheric and solar disturbances. Both orbital and spectral congestion are a threat to links (as well as to satellites).[10] Such congestion may restrict the future use of potential orbits and frequencies and cause unintentional interference to satellite services. According to one commercial service provider, satellite service providers worldwide work together to resolve interference problems, which are common. In addition, commercial satellite interference is regulated both internationally and nationally. The International Telecommunication Union specifies interference resolution policies and procedures, including those for harmful interference.[11] Further, within the United States, the Federal Communications Commission (FCC)[12] has the capability to track the location of interference, at a service provider's request. Also, service providers told us that they could locate and identify unintentional or unauthorized users through a technique called triangulation. Once an unauthorized user is located, a commercial service provider can jam that user's signal if the user cannot be persuaded to stop using the satellite. However, according to industry officials, typically an unauthorized user would be identified, located, and contacted through a combination of industry and government resources before such jamming would be needed.

In addition, satellite systems are vulnerable to many forms of intentional human attacks that are intended to destroy ground stations and satellites or interfere with the TT&C links, data links, and cross-links. According to DOD and the private sector, the probability of these threats occurring and

[10] The greatly increasing number of commercial and military communications systems worldwide, including the growing number of satellites, is putting a high demand on certain frequency spectra. Orbital/spectral congestion may restrict the future use of potential orbits and frequencies, further complicate and lengthen host nation approval and landing rights processes, and require more sophisticated systems in terms of frequency agility, antennas, bandwidth-efficient modulation, and so forth to maximize flexibility. Such flexibility minimizes future risks arising from changes in spectrum allocation and the electromagnetic environment.

[11] The International Telecommunication Union is an international organization within the United Nations system in which governments and the private sector work together to coordinate the operation of telecommunication networks and services and advance the development of communications technology.

[12] The Federal Communications Commission is an independent U.S. government agency. The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite, and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions.

the difficulty of exploiting these vulnerabilities vary. Table 3 shows some of these intentional threats.

Table 3: Intentional Threats to Commercial Satellite Systems

Type of threat	Vulnerable satellite system components
Ground-based:	
Physical destruction	Ground stations; communications networks
Sabotage	All systems
Space-based (anti-satellite):	
Interceptors (space mines and space-to-space missiles)	Satellites
Directed-energy weapons (laser energy, electromagnetic pulse)	Satellites; TT&C and data links
Interference and content-oriented:	
Cyber attacks (malicious software, denial of service, spoofing, data interception, and so forth)	All systems and communications networks
Jamming	All systems

Source: GAO analysis.

All types of ground stations are potentially vulnerable to threats of physical attack and sabotage. These threats could target all satellite ground components, including launch facilities, command and control facilities, and supporting infrastructures.

Space-based threats to satellites are proliferating as a result of the growing availability of technology around the world. According to DOD, potential space-based weapons include interceptors, such as space mines and orbiting space-to-space missiles, and directed-energy weapons. Directed-energy weapons include ground-based, airborne, and space-based weapons that use laser energy to damage or destroy satellite services, and nuclear weapons that generate nuclear radiation and electronic pulses, resulting in direct damage to the orbital electronics by the primary and secondary effects of a detonation.

Ground stations, links, and supporting communications networks are all vulnerable to cyber attacks. Potential cyber attacks include denial of service, malicious software, unauthorized monitoring and disclosure of sensitive information (data interception), injection of fake signals or traffic ("spoofing"), and unauthorized modification or deliberate corruption of network information, services, and databases. For example, malicious software (such as computer viruses) can be (1) implanted into computer systems during development or inserted during operations; (2) used to manipulate network protocols, deny data or service, destroy data or software, and corrupt, modify, or compromise data; and (3) used to attack processor-controlled transmission equipment, control systems, or the information being passed.

Links are particularly susceptible to electronic interference threats capable of disrupting or denying satellite communications. These threats include spoofing and jamming. A spoofer emits false, but plausible, signals for deception purposes. If false commands could be inserted into a satellite's command receiver (spoofing the receiver), they could cause the spacecraft to tumble or otherwise destroy itself. It is also feasible to insert false information or computer viruses into the terrestrial computer networks associated with a space system, either remotely or through an on-site connection. Such an attack could lead to space system degradation or even complete loss of spacecraft utility.

A jammer emits noise-like signals in an effort to mask or prevent the reception of desired signals and can be used to disrupt uplinks, downlinks, and cross-links. An uplink jammer attempts to inject noise or some other signal into the targeted satellites' uplink receivers. In general, an uplink jammer must be roughly as powerful as the emitter associated with the link being jammed.

Downlink jamming attempts to inject noise or some other signal directly into earth terminal receivers. The targets of downlink jammers are ground-based satellite data receivers, ranging from large fixed ground sites to handheld Global Positioning System (GPS) user terminals. Since downlink jammers have a range advantage over the space-based emitters, they can often be much less powerful. Downlink jamming is generally easier to accomplish than uplink jamming, since very low-power jammers are often suitable. Since a downlink may be received by multiple earth terminals, it is often more difficult to jam more than a few earth terminals through downlink jamming than through uplink jamming, especially if the receiver terminals are dispersed across a significant geographical area.

A cross-link jammer attempts to inject noise or some other signal between two satellites communicating directly with each other. Because it is considered the most complex and difficult approach to satellite jamming, according to a DOD document,[13] cross-link jamming is considered a lower probability threat than uplink and downlink jamming.

Satellite Vulnerabilities Have Led to Disruptions

Satellite services have been disrupted or denied as a result of system vulnerabilities. Below is a list of satellite-related incidents that have been publicly reported in which services were interrupted unintentionally or intentionally because of satellites' vulnerabilities to jamming and equipment failure:

- In April 1986, an insider, working alone under the name "Captain Midnight" at a commercial satellite transmission center in central Florida, succeeded in disrupting a cable network's eastern uplink feed to the Galaxy I satellite. Although this event was a minor annoyance, it had the potential for disrupting services to satellite users.

- Starting in 1995, MED-TV, a Kurdish satellite channel, was intentionally jammed (and eventually had its license revoked) because its broadcasts promoted terrorism and violence.

- In 1997, while a GPS transmitter was being tested on the ground, it unintentionally interfered with the GPS receivers of a commercial aircraft in the area. The plane temporarily lost all of its GPS information.

- In 1997, Indonesia intentionally interfered with and denied the services of a commercial satellite belonging to the South Pacific island kingdom of Tonga because of a satellite orbital slot dispute.

- In 1998, the failure of PANAMSAT's Galaxy IV satellite, attributable to an on-board processor anomaly, disabled 80 to 90 percent of 45 million pagers across the United States for 2 to 4 days, leaving approximately 70 percent of a major oil company's customers without the ability to pay for services at the pump.

[13] Department of Defense, *Advanced Military Satellite Communications Capstone Requirements* (Colorado Springs, Colo.: Apr. 24, 1998).

Critical Infrastructure Protection Policy Addresses Information Security of Key Sectors

Recognizing that our nation's critical infrastructures, including telecommunications, energy, banking and finance, transportation, and satellites, are the foundation of our economy, national security, and quality of life, in October 1997 the President's Commission on Critical Infrastructure Protection issued a report recommending several measures to achieve a higher level of protection of critical infrastructures. These measures included industry cooperation and information sharing, the creation of a national organization structure, a revised program of research and development, a broad program of awareness and education, and reconsideration of laws related to infrastructure protection. The report also described the potentially devastating implications of poor information security from a national perspective. The report stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyber threats."[14]

Presidential Decision Directive (PDD) 63, issued in 1998 to improve the federal government's approach to critical infrastructure protection (CIP), describes a strategy for cooperative efforts by government and the private sector to protect critical computer-dependent operations. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved, and it designated lead agencies to work with private-sector and government entities. To accomplish its goals, PDD 63 designated and established organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office that is housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies; and
- the National Infrastructure Protection Center, an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response.

[14] Report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (October 1997).

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures and five special functions; information and communication is one of the eight infrastructures identified. Further, the directive designated lead federal agencies to work with the private-sector entities. For example, Commerce is the lead agency for the information and communication sector (the responsible organization within Commerce is the National Telecommunications and Information Administration), and the Department of Energy is the lead agency for the electrical power industry. Similarly, for special function areas, DOD is responsible for national defense, and the Department of State is responsible for foreign affairs.

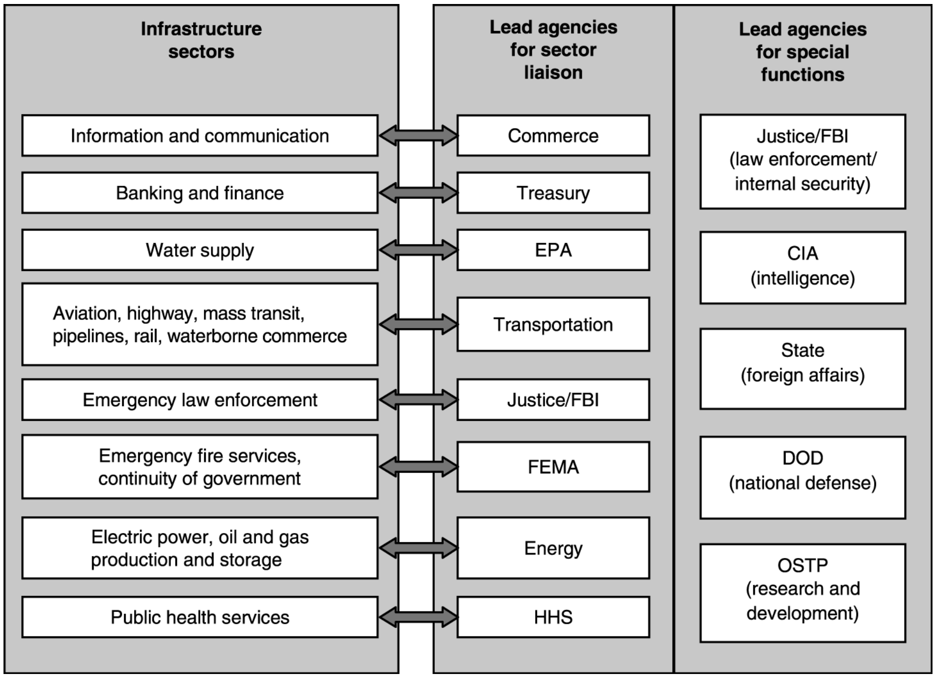
To facilitate private-sector participation, PDD 63 also encouraged creation of information sharing and analysis centers (ISACs) that could serve as a mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through the FBI's National Infrastructure Protection Center.[15] Although most of the ISACs are operated by private-sector organizations, the telecommunications ISAC is operated by a government entity, the National Coordinating Center for Telecommunications (NCC), which is part of the National Communications System.[16] In September 2001, we reported that six ISACs within five infrastructures had been established to gather and share information about vulnerabilities, attempted intrusions, and attacks within their respective infrastructure sectors and to meet specific sector objectives.[17] In addition, at that time, we reported that the formation of at least three more ISACs for various infrastructure sectors was being discussed. Figure 2 displays a high-level overview of several organizations with CIP responsibilities, as outlined by PDD 63.

[15] See U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001) for our latest report on the progress of the National Infrastructure Protection Center.

[16] In 1963, the National Communications System was established by presidential memorandum as a federal interagency group responsible for national security and emergency preparedness telecommunications. These responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure, which now includes the Internet, to achieve effectiveness in managing and using national telecommunication resources to support the federal government during any emergency.

[17] U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: Sept. 20, 2001).

Figure 2: Entities with CIP Responsibilities as Outlined by PDD 63



Infrastructure sectors	Lead agencies for sector liaison
Information and communication	Commerce
Banking and finance	Treasury
Water supply	EPA
Aviation, highway, mass transit, pipelines, rail, waterborne commerce	Transportation
Emergency law enforcement	Justice/FBI
Emergency fire services, continuity of government	FEMA
Electric power, oil and gas production and storage	Energy
Public health services	HHS

Lead agencies for special functions

Justice/FBI (law enforcement/ internal security)

CIA (intelligence)

State (foreign affairs)

DOD (national defense)

OSTP (research and development)

Source: CIAO.

The most recent federal cyber CIP guidance was issued in October 2001, when President Bush signed Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, which continues many PDD 63 activities by focusing on cyber threats to critical infrastructures and creating the President's Board on CIP to coordinate cyber-related federal efforts. The Special Advisor to the President for Cyberspace Security chairs the board.

In July 2002, the President issued a national strategy for homeland security that identifies 14 industry sectors, including the 8 identified in PDD 63. The additional 6 are agriculture, food, defense industrial base, chemical industry and hazardous materials, postal and shipping, and national monuments and icons.[18]

[18] Office of Homeland Security, *National Strategy for Homeland Security* (July 2002).

Current Space Policy Addresses Aspects of Federal Uses of Commercial Satellites

The U.S. national space policy provides goals and guidelines for the U.S. space program, including the use of commercial satellites. In February 1991, the President issued National Space Policy Directive 3, which requires U.S. government agencies to use commercially available space products and services to the fullest extent feasible. Presidential Decision Directive 49, dated September 19, 1996, provides goals for the U.S. space program and establishes space guidelines. For example, a guideline regarding the commercial space industry stated that U.S. government agencies shall purchase commercially available space goods and services to the fullest extent feasible, and that, except for reasons of national security or public safety, they shall not conduct activities with commercial applications that preclude or deter commercial space activities. Neither the National Space Policy Directive 3 nor PDD 49 specifically addresses the security of satellite systems used by federal agencies. However, PDD 49 states that critical capabilities necessary for executing space missions must be ensured. Security of satellite systems has been addressed in policy documents issued by the National Security Telecommunications and Information Systems Security Committee (recently renamed the Committee on National Security Systems). The initial policy was set forth in *National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems*, *National Telecommunications and Information Systems Security Policy (NTISSP) No. 1* (June 17, 1985), which governed the protection of command and control uplinks for government-used satellites other than military. This policy, which applies to space systems launched 5 years from the policy date (June 17, 1985), limits government and government contractor use of U.S. civil and commercial satellites to those systems using accepted techniques to protect the command and control uplinks.

In January 2001, a new policy governing satellite system security was issued, superseding NTISSP No. 1: *National Information Assurance (IA) Policy for U.S. Space Systems*, *National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 12*. NSTISSP No. 12, which focuses on systems used for U.S. national security information, aims to ensure that information assurance[19] is factored into "the planning, design, launch, sustained operation, and deactivation of

[19] Information assurance refers to information operations intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

federal and commercial space systems used to collect, generate, process, store, display, or transmit and receive such information." The policy also includes a provision addressing commercial imagery satellites that may be used to satisfy national security requirements during periods of conflict or war. The policy states that approved U.S. cryptographies shall be used to provide confidentiality for (1) command and control uplinks, (2) data links that transmit national security information between the ground and the space platforms, (3) cross-links between space platforms, and (4) downlinks from space platforms to mission ground or processing centers.[20]

Security Techniques Are Available to Protect TT&C and Data Links, Satellites, and Ground Stations

A range of security techniques is available for protecting satellite systems: for example, using encryption on TT&C and data links, using robust parts on the satellites, and applying physical and cyber security controls at the ground stations. The application of these techniques varies across federal agencies and the private sector. Commercial satellite service providers typically use some of these security techniques to meet most of their customers' security requirements, and they base their decisions on business objectives. Generally, the military applies more stringent security techniques to their satellites than do civilian agencies or the private sector. Table 4 provides an overview of security techniques by satellite system component.

[20] Approved U.S. cryptographies are hardware, firmware, or software implementations of algorithms that have been reviewed and approved by the National Security Agency, the purposes of which are to provide authentication or confidentiality for national security information or systems.

Table 4: Security Techniques Available to Address Unintentional and Intentional Threats

Satellite system components	Security techniques available	Type of threat addressed
TT&C and data links	Encryption	Cyber attacks
	High-power radio frequency (RF) uplink	Jamming
	Spread spectrum	Jamming
	Unique digital interface	Cyber attacks, jamming
Satellites	Hardening	Space environment, interceptors, directed-energy weapons
	Redundancy	Sabotage, space objects, interceptors, directed-energy weapons
Ground stations	Physical and logical security controls	Physical destruction, sabotage, cyber attacks, jamming, power outages
	Hardening	Natural occurrences, physical destruction, cyber attacks, jamming
	Redundancy	Natural occurrences, physical destruction, sabotage, power outages

Source: GAO analysis.

Various Techniques Can Protect TT&C and Data Links

Techniques to protect satellite links include the use of encryption, high-power radio frequency (RF) uplinks, spread spectrum communications, and a digital interface unique to each satellite. Commercial satellite service providers, federal satellite owners and operators, and customers stated that they typically use at least one of these techniques. Usually, only the military uses spread spectrum techniques.

Both TT&C and data links can be protected by encryption: generally, for TT&C links, the tracking and control uplink is encrypted, while the telemetry downlink is not. Encryption is the transformation of ordinary data (commonly referred to as plaintext) into a code form (ciphertext) and back into plaintext, using a mathematical process called an algorithm. Encryption can be used on data to (1) hide information content, (2) prevent undetected modification, and (3) prevent unauthorized use.

Different levels of encryption provide different levels of protection, including encryption approved by the National Security Agency (NSA) that is used for national security information. NSTISSP No. 12 requires approved U.S. cryptographies on TT&C and data links for U.S. space systems transmitting national security information. For satellite systems transmitting non–national-security information, there is no policy that security is required for the links, but satellite service providers and federal satellite owners and operators included in our review stated that they protect tracking and control uplinks with encryption. However, NSA officials stated that not all commercial providers' tracking and control uplinks are encrypted. Concerning the data links, customers are responsible for determining whether they are encrypted or not. Most commercial satellite systems are designed for "open access," meaning that a transmitted signal is broadcast universally and unprotected.

A second security technique for links is the use of high-power RF uplinks: that is, a large antenna used to send a high-power signal from the ground station to the satellite. To intentionally interfere with a satellite's links, an attacker would need a large antenna with a powerful radio transmitter (as well as considerable technical knowledge). Two of the commercial providers we talked to stated that they use high-power RF uplinks as part of their satellite security approach. According to one commercial provider, most satellite operators use high-power RF uplinks for TT&C connections to block potential unauthorized users' attempts to interfere with or jam the TT&C uplink.

A third technique for protecting links is the use of spread spectrum communication, a technique used by the military and not normally implemented by commercial providers. Spread spectrum communication is a form of wireless communication in which the frequency of the transmitted signal is deliberately varied and spread over a wide frequency band. Because the frequency of the transmitted signal is deliberately varied, spread spectrum communication can provide security to links because it increases the power required to jam the signals even if they are detected. Spread spectrum communication is primarily used to optimize the efficiency of bandwidth within a frequency range, but it also provides security benefits.[21]

Finally, TT&C links can be protected by the use of a unique digital interface between the ground station and the satellite. According to one commercial

[21] Two desired outcomes of using spread spectrum communications as a security technique are low probability of intercept and low probability of detection, which increase the difficulty of detecting and jamming signals. These outcomes, although not mentioned by entities in our review, require that the transmission occur in quick, random bursts to make it harder to detect, and that the signal is narrowed to make it harder to intercept. In contrast, most commercial satellites have a wide beam and continuous coverage, so that as many customers as possible can be covered by a limited number of satellites, thus driving up return on investment.

satellite service provider, most commercial providers use a unique digital interface with each satellite. Tracking and control instructions sent from the ground station to the satellite are encoded and formatted in a way that is not publicly known. Officials from the commercial satellite vendor stated that even if an attacker were successful in hacking one satellite, the unique interface could prevent the attacker from taking control of an entire fleet of satellites. In addition, communication with the digital interface to the tracking and control links requires high transmission power, so that an attacker would need a large, powerful antenna.

Satellites Can Be Protected through Hardening and Redundancy

Satellites can be protected by (1) "hardening," through designs and components that are built to be robust enough to withstand harsh space environments and deliberate attacks, and (2) the use of redundancy—backup systems and components. Commercial satellite service providers and federal civilian owners and operators told us that they do not harden their satellites to the extent that the military does. Commercial providers, federal civilian owners and operators, and the military use varying degrees of redundancy to protect their satellites.

As satellites rely increasingly on on-board information processing, hardening is becoming more important as a security technique. Hardening in this context includes physical hardening and electronic-component hardening. Satellites can be hardened against natural environmental conditions and deliberate attack, and to ensure survivability.[22] Most hardening efforts are focused on providing sufficient protection to electronic components in satellites so that they can withstand natural environmental conditions over the expected lifespan of the satellite, which could be nearly 15 years. For hardening against deliberate attacks, some techniques proposed include the use of reflective surfaces, shutters, and nonabsorbing materials. According to commercial satellite providers, commercial satellites are not normally hardened against non-natural nuclear radiation because it is too costly. The drawback of hardening is the cost and the manufacturing and operational burdens that it imposes on satellite manufacturers and providers.

[22] Survivability is the property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance, as for example a nuclear burst.

The use of high-quality space parts is another approach to hardening. Although all parts used in satellites are designed to withstand natural environmental conditions, some very high-quality parts that have undergone rigorous testing and have appreciably higher hardness than standard space parts are also available, including those referred to as class “S” parts. These higher quality space parts cost significantly more than regular space parts—partly because of the significant testing procedures and more limited number of commercial providers manufacturing hardened parts. According to an industry official, high-quality space parts are used by the military and are generally not used on commercial satellites.

Commercial satellite providers stated that they also use redundancy to ensure availability, through backup satellites and redundant features on individual satellites. Backup satellites enable an organization to continue operations if a primary satellite fails. One provider stated that it would rather spend resources on backup satellites than on hardening future satellites or encrypting the TT&C and data links. The provider also expressed the view that a greater number of smaller, less costly satellites provides greater reliability than is provided by few large satellites, because there is more redundancy. According to an industry consulting group, backup satellites, which include in-orbit and on-ground satellites, are part of commercial satellite providers’ security approaches. When backup satellites are used, they are commonly kept in orbit; keeping backup satellites on the ground is possible, but it has the disadvantage that the system cannot immediately continue operations if the primary satellite fails. According to one provider, it could take 4 to 6 months to launch a backup satellite stored on the ground.

In addition, individual satellites can be designed to have redundant parts. For example, a commercial satellite provider told us that redundant processors, antennas, control systems, transponders, and other equipment are frequently used to ensure satellite survivability. Another example is that satellites could have two completely separate sets of hardware and two paths for software and information; this is referred to as having an A-side and a B-side. In general, this technique is not used on commercial satellites, according to an industry official.

Ground Stations Can Be Protected Primarily by Physical Security Controls

Techniques to protect ground stations include physical controls as well as logical security controls, hardening, and backup ground stations. Ground stations are important because they control the satellite and receive and process data. One provider stated that providing physical security measures to ground stations is important because the greatest security threat to satellite systems exists at that location.

Locations of ground stations are usually known and accessible; thus, they require physical security controls such as fencing, guards, and internal security. One provider emphasized the importance of performing background checks on employees. Civilian agencies also stated that they protected ground stations through various physical security controls: ground stations are fenced, guarded, and secured inside with access control devices, such as key cards.

The commercial satellite service providers included in our review stated that they did not protect their ground stations through hardening; this technique is primarily used by the military.[23] Similarly, most civilian agencies we talked to do not harden their ground stations. A ground station would be considered hardened if it had protective measures to enable it to withstand destructive forces such as explosions, natural disasters, or ionizing radiation.

Commercial satellite providers and federal agency satellite owners and operators also may maintain off-line or fully redundant ground stations to ensure availability, which can be used if the primary ground station is disrupted or destroyed. Off-line backup ground stations may not be staffed or managed by the same company, or on a full-time basis. In addition, off-line backup ground stations are not necessarily designed for long-term control of satellites. On the other hand, one commercial service provider stated that it maintained fully redundant, co-primary, geographically separated ground stations that are fully staffed with trained operators, gated with restricted access, and capable of long-term uninterruptible power. In addition, these ground stations periodically alternated which satellites they were responsible for as a training exercise. They also operated 24 hours a day, 7 days a week, and monitored each other.

[23] Hardening of ground stations includes robust physical security features like blast resistant physical structures and radomes to protect antennas.

Federal Satellite Users Can Reduce Risks Only in Certain Areas, and National Policy Is Limited

To mitigate the risk associated with using commercial satellites, federal agencies focus on areas within their responsibility and control: data links and communication ground stations. According to federal agency officials, agencies reduce risks associated with using commercial satellites by (1) protecting the data's authentication and confidentiality with encryption, (2) securing the data ground stations with physical security controls and backup sites, and (3) ensuring service availability through redundancy and dedicated services. Federal agencies rely on commercial satellite service providers to provide the security techniques for the TT&C links, satellites, and satellite control stations. However, federal agency officials stated that they were unable to impose specific security requirements on commercial satellite service providers. Further, federal policy governing the security of satellite systems used by agencies is limited because it addresses only those satellites used for national security information, pertains only to techniques associated with the links between ground stations and satellites and between satellites (cross-links), and does not have an enforcement mechanism. Without appropriate governmentwide policy to address the security of all satellite components and of non–national-security information, federal agencies may not, for information with similar sensitivity and criticality, consistently (1) secure data links and communication ground stations or (2) use satellites that have certain security controls that enhance availability. Recent initiatives by the Executive Branch have acknowledged these policy limitations, but we are not aware of specific actions to address them.

Agencies Provide Encryption to Protect Data

For critical data, agencies primarily use different types of encryption to reduce the risk of unauthorized use or changes. For example, the military services use encryption to protect most data communicated over satellites—either commercially owned or military. DOD officials stated that the military services use the strongest encryption algorithms available from the NSA for the most sensitive information—national security information. For non–national-security information, the military services use less strong encryption algorithms, according to DOD officials. The National Aeronautics and Space Administration (NASA) also uses NSA-provided encryption for critical operations, such as human mission communications (that is, for space shuttle missions). Using NSA encryption requires encryption and decryption hardware at the data's source and destination, respectively. The use of this hardware requires agencies and satellite service providers to apply special physical protection procedures—such as restricting access to the equipment and allowing no access by foreign nationals. For the next generation of government-owned weather satellites, the National Oceanic and Atmospheric Administration (NOAA) and the U.S. military plan to use an NSA-approved commercial encryption package that will avoid the need for special equipment and allow them to restrict the data to authorized users with user IDs and passwords. In addition, NOAA will be able to encrypt broadcast weather data over particular regions of the world.

According to NASA and NOAA officials, some agency data do not require protection because the risk of unauthorized use or changes is not significant or because the information is intended to be available to a broad audience. For example, NASA uses satellites to provide large bandwidth to transmit scientific data from remote locations. According to NASA officials, the agency does not protect the transmission of these data because they are considered academic in nature and low risk. In addition, the Federal Aviation Administration (FAA) does not encrypt links between control centers or between control centers and aircraft, because the data on these links go from specific air traffic control centers to specific aircraft. According to FAA officials, if the transmissions were required to be encrypted, every aircraft would have to acquire costly decryption equipment. Further, according to National Weather Service officials, the service does not protect the weather data transmitted over commercial satellites because the service considers it important to make this information widely available not only to its sites but also to government agencies, commercial partners, universities, and others with the appropriate equipment.

Agencies Provide Physical Security for Communications Ground Stations

Federal agencies also control the security of the data ground stations that send and receive data over satellites. To protect these ground stations, federal officials stated that they use physical security techniques, such as those discussed earlier. They protect their facilities and equipment from unintentional and intentional threats (such as wind, snow, and vandalism). For example, according to FAA officials, in certain locations, FAA has hardened remote satellite ground stations against high wind and cold weather conditions. In addition, NOAA officials stated that many of their antennas are hurricane protected. Further, federal officials stated that they perform background checks on personnel. NOAA officials stated that they perform background checks on satellite technicians to the secret clearance level. Federal officials also stated that their ground stations are further protected because they are located on large, protected federal facilities. For example, military ground stations can be located on protected U.S. or allied military bases. Also, National Weather Service officials stated that the service's primary communications uplink is located on a highly secured federal site. Further, according to DOD officials, personnel are expected to protect the satellite equipment provided to them in the field. Agencies also had backup communications sites that were geographically separated, including being on different power grids. For example, according to an official, the National Weather Service's planned backup communications uplink site will be geographically separated from the primary site and will be on a secured federal site.

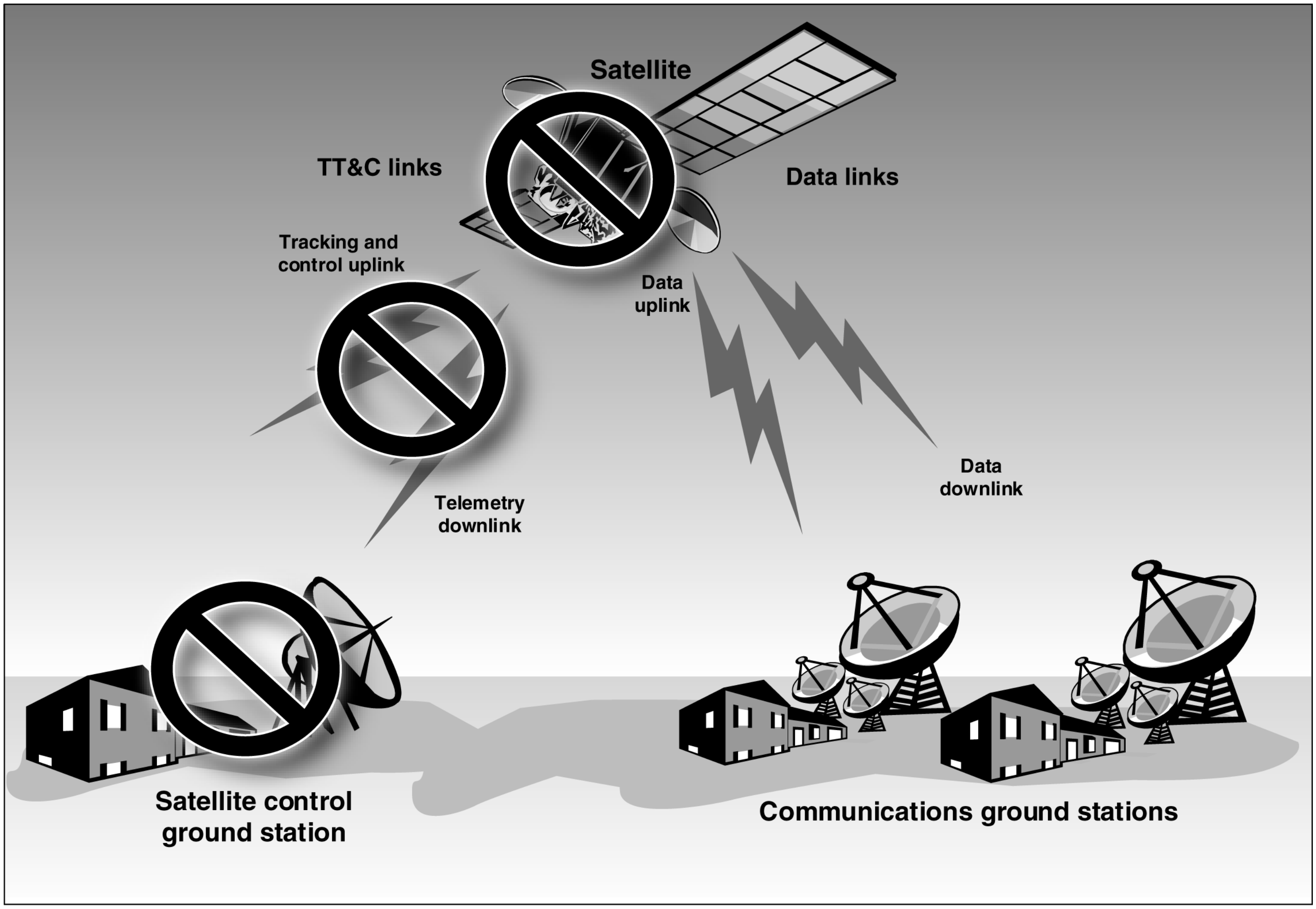
Agencies Attempt to Ensure Availability through Redundancy and Dedicated Services

Federal agencies also reduce the risk associated with using commercial satellites by having redundant telecommunications capabilities. For example, for the program that provides Alaska's air traffic control, FAA relies on two satellites to provide backup capacity for each other. In addition to this redundancy, FAA has requested its commercial satellite service provider to preferentially provide services to FAA's Alaska air traffic control system over other customers carried on the same satellites. Another FAA program provides primary communications capabilities in remote locations and has redundant satellite capacity that can be used if the primary satellite fails. The National Weather Service is another example. The service uses redundancy to ensure the availability of satellite services that broadcast weather data to its 160 locations by contracting for priority services that include guarantees of additional transponders or, if the satellite fails, of services on other satellites. In addition, the service plans to own and operate a backup communications center that is geographically separated from the primary site. The service performs monthly tests of the backup site's ability to provide the communications uplink to the commercial satellites.

Agencies Do Not Control All Aspects of Security and Have Limited Ability to Influence Availability and Security Requirements

Federal agencies rely on the commercial satellite service provider's security techniques for the TT&C links, satellites, and satellite control ground stations. Figure 3 graphically depicts the areas not controlled by federal agencies.

Figure 3: Commercial Satellite System Showing Components Not Controlled by Government Agencies


Satellite
TT&C links
Data links
Tracking and control uplink
Data uplink
Telemetry downlink
Data downlink
Satellite control ground station
Communications ground stations

🛇 Satellite components not controlled by federal agencies

Source: GAO analysis.

To mitigate the risk associated with not controlling aspects of commercial satellite security other than protecting the data links and communications ground stations, federal agencies attempt to specify availability[24] and reliability[25] requirements, but they acknowledge having had limited influence over security techniques employed by commercial satellite service providers.[26] Federal officials stated that they are usually constrained by the availability and reliability levels that can be provided by their telecommunications service providers. For example, for one program, an FAA contract requires 99.7 percent availability in recognition of the satellite service provider's limitations, though the agency typically receives 99.8 percent. However, FAA would prefer 99.999 percent availability on this program's satellite communications, which is similar to the reliability level being received from terrestrial networks that FAA uses where available. According to one FAA official, greater satellite reliability could be gained by having multiple satellite service providers furnish communications over the same regions, but this approach is too costly.

Although maintaining established or contracted reliability levels generally requires that service providers maintain some level of security, federal officials stated that their agencies cannot usually require commercial satellite service providers to use specific security techniques. Commercial satellite service providers have established operational procedures, including security techniques, some of which, according to officials, cannot be easily changed. For example, once a satellite is launched, additional hardening or encryption of the TT&C link is difficult, if not impossible. Some service providers offer the capability to encrypt the command uplinks. According to FAA officials, FAA is in the process of performing risk assessments, in compliance with its own information systems security policies, on the commercial services (including satellite services) that it acquires. Based on these risk assessments, FAA officials plan to accredit

[24] Availability is the ratio of the total time a service is being used during a given interval to the length of the interval. For example, a service provider may state that its services will be available 99.99 percent over a year, which amounts to 53 minutes of accumulated outages for all causes over the course of the year. Additional decimal places, such as 99.999 percent, represent greater levels of availability. Federal Telecommunications Standards Committee, *Telecom Glossary 2000* (Feb. 2, 2001).

[25] Reliability is the probability that a service will perform its required function for a specified period of time under stated conditions. Federal Telecommunications Standards Committee, *Telecom Glossary 2000* (Feb. 2, 2001).

[26] Security is one of many factors that affect satellite availability and reliability. Others include weather and power outages.

and certify the security of the agency's program that relies on commercial satellites.

Existing Federal Policy Concerning Commercial Satellite Security Is Limited

Federal policy governing agencies' actions regarding the security of commercial satellite systems is limited, in that it (1) pertains only to satellites used for national security purposes, (2) addresses security techniques associated with links only, and (3) does not have an enforcement mechanism for ensuring compliance. Although the Executive Branch has recently acknowledged these policy limitations, we are not aware of specific actions to address them.

NSTISSP No. 12, the current policy governing satellite system security, applies only to U.S. space systems (U.S. government-owned or commercially owned and operated space systems) that are used for national security information and to imagery satellites that are or could be used for national security purposes during periods of conflict or war. It does not apply to systems that process sensitive, non–national-security information. Issued by the National Security Telecommunications and Information Systems Security Committee (now the Committee on National Security Systems (CNSS)), NSTISSP No. 12 has as its primary objective "to ensure that information assurance is factored into the planning, design, launch, sustained operation, and deactivation of U.S. space systems used to collect, generate, process, store, display, or transmit/receive national security information, as well as any supporting or related national security systems." NSTISSP No. 12 also suggests that federal agencies may want to consider applying the policy's information assurance requirements to those space systems that are essential to the conduct of agencies' unclassified missions, or to the operation and maintenance of critical infrastructures.

In addition to having a focus only on national security, the policy is further limited in that it addresses security techniques only for the links. It does not include physical security requirements for the satellites or ground stations. Specifically, for satellite systems to which it applies, NSTISSP No. 12 states that approved U.S. cryptographies shall be used to provide confidentiality for the (1) command and control uplinks, (2) data links that transmit national security information between the ground and the space platforms, (3) cross-links between space platforms, and (4) downlinks from space platforms to mission ground or processing centers.

Also, there is no enforcement mechanism to ensure agency compliance with the policy. According to one NSA official on the CNSS support staff, enforcement of such policies has always been a problem, because no one has the authority to force agencies' compliance with them. According to some agency officials, agencies typically do not test their service providers' implementation of security procedures.

According to the federal and commercial officials involved in our study, no commercial satellite is currently fully compliant with NSTISSP No. 12, and gaining support to build compliant systems would be difficult. According to commercial satellite industry officials, there is no business case for voluntarily following the NSTISSP No. 12 requirements and implementing them in the satellites and ground stations, including networks that are currently being developed.

Commercial satellite service providers also raised concerns about the impact of NSTISSP No. 12 on their future commercial satellite systems. Several officials stated that if compliance were required, it would significantly increase the complexity of managing the satellites, because encryption key management is cumbersome,[27] and appropriately controlling access to the hardware is difficult in global companies that have many foreign nationals. Also, commercial satellite service providers stated that encrypting the TT&C links could increase the difficulty of troubleshooting, for example, because the time it takes to encrypt and then decrypt a command could become significant when a TT&C problem arises. Other issues raised that make NSTISSP No. 12 difficult to implement include the following:

- Some satellite service providers view compliance with it as not necessary for selling services to the government, since in the past agencies have used satellites that did not comply with prior security policy. For example, DOD has contracted for services on satellites that were not compliant with the previous and existing policy for various reasons. However, at times, noncompliant satellites have been DOD's only option.

- Commercial clients will likely be unwilling to pay the additional cost associated with higher levels of encryption. Significant costs would include licensing agreements and redesigning hardware for new encryption technologies.

[27] A key is a special value associated with an encryption algorithm that is used for coding and decoding.

- Satellite industry officials stated that their experience shows that encryption does not really provide much greater security than other techniques that protect TT&C and data links.

Notwithstanding the above issues, in response to the policy's limitations, DOD officials from the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence stated that the department had started drafting a policy that would require all commercial satellite systems used by DOD to meet NSTISSP No. 12 requirements. This draft policy includes a waiver process requiring prior approval before any satellite system could be used that did not meet the security requirements. If approved, this policy would apply only to DOD. DOD officials are anticipating that this policy will be approved by the end of 2002.

In addition to DOD's efforts, a CNSS official stated that a draft policy was developed to address the lack of national policy or guidance for the assurance of non–national-security information. Although this policy was broad in scope, covering many aspects of information assurance, this official stated that satellite security could be included in its scope. However, this official also stated that the CNSS's efforts ended in April 2002 when it sent the draft policy to the Director of the Office of Management and Budget (OMB) for consideration, because the CNSS lacks authority in the area of non–national-security information. In transmitting the draft policy to the Director, OMB, the CNSS Chair encouraged the development of this policy as a first step in establishing a national policy addressing the protection of information technology systems that process sensitive homeland security information, as well as information associated with the operation of critical infrastructures. According to an OMB official, the draft policy is valuable input for future policy decisions related to protecting government information.

Recognizing that space activities are indispensable to our national security and economic vitality, on May 8, 2002, the President's National Security Advisor sent a memorandum to top cabinet officials stating that she plans to recommend that the White House initiate a review of U.S. space policies that have been in place since 1996. To date, we are not aware of specific actions taken in response to the draft policy sent to OMB and the National Security Advisor's memorandum.

Without appropriate governmentwide policy to address the security of all satellite components and of non–national-security information, federal agencies may not, for information with similar sensitivity and criticality, consistently (1) secure data links and communication ground stations or (2) use satellites that have certain security controls that enhance availability. As a result, federal agencies risk losing needed capabilities in the event of the exploitation of satellite system vulnerabilities.

National CIP Initiatives Addressing Satellite Security Have Been Limited

PDD 63 was issued to improve the federal approach to protecting our nation's critical infrastructures by establishing partnerships between private-sector entities and the federal government. Although this directive addressed the satellite vulnerabilities of GPS and led to a detailed vulnerability assessment, the satellite industry has not received focused attention as part of this national effort. Given the importance of commercial satellites to our nation's economy, the federal government's growing reliance on them, and the dependency of many other infrastructures on satellites, not including them in our national CIP approach creates the risk that these critical components of our information and communication infrastructure may not receive needed attention.

Both PDD 63 and the report of the President's Commission on Critical Infrastructure Protection (October 1997) addressed satellite vulnerabilities of the GPS and made several recommendations to the Secretary of Transportation, including to fully evaluate these vulnerabilities and actual and potential sources of interference to the system. In August 2001, the John A. Volpe Transportation Systems Center issued a report that includes an assessment of the vulnerabilities of the GPS; analysis of civilian aviation, maritime, and surface uses; assessment of the ways that users may be affected by short- or long-term GPS outages; and recommendations to minimize the safety and operational impacts of such outages.[28] One overarching finding was that because of the increasing reliance of transportation on GPS, the consequences of loss of the signal could be severe in terms of safety and of environmental and economic damage to the nation.

Despite the focused attention on GPS, other aspects of the satellite industry have not received national attention. In PDD 63, commercial satellites were not identified as a critical infrastructure (or as part of one), and thus are not specifically included as part of our nation's approach to

[28] John A. Volpe National Transportation Systems Center, *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System: Final Report* (Aug. 29, 2001).

protecting critical infrastructures. Further, PDD 63 does not explicitly include the commercial satellite industry as part of the information and communications infrastructure sector, nor does the newly issued national strategy for homeland security. Although there have been discussions about expanding the coverage of individual sectors (particularly since the events of September 11, 2001), National Telecommunications and Information Administration (NTIA) officials stated that there are no specific plans to build better partnerships with satellite builders and operators as part of their efforts. CIAO officials also told us that there are no specific plans to include commercial satellite companies in current national efforts. However, CIAO added that some of the current infrastructure sectors may address satellites in their plans for industry vulnerability assessments and remediation, since some of these infrastructures rely on satellites for communications or other functions, such as tracking shipments or trucks, or monitoring the condition of equipment. The telecommunications ISAC reiterated NTIA's and CIAO's comments that there are no specific plans to include satellites in national CIP efforts. The ISAC for the telecommunications sector, recognized by the President's National Security Council in January 2000, is the National Coordinating Center for Telecommunications (NCC), which is operated by the National Communications System. As such, NCC is responsible for facilitating the exchange of information among government and industry participants regarding computer-based vulnerability, threat, and intrusion information affecting the telecommunications infrastructure. Also, the center analyzes data received from telecommunications industry members, government, and other sources to avoid or lessen the impact of a crisis affecting the telecommunications infrastructure. Since its recognition as an ISAC, NCC membership has expanded beyond traditional telecommunications entities to include some aerospace companies such as Boeing and Raytheon, but the ISAC does not specifically focus on commercial satellites.

Officials from one of the satellite service providers told us that they would endorse an ISAC-like forum to discuss vulnerabilities to commercial and military satellites. In July 2002, we recommended that when developing the strategy to guide federal CIP efforts, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the Special Advisor to the President for Cyberspace Security ensure, among other things, that the strategy includes all relevant sectors and defines the key federal agencies' roles and responsibilities associated with each of these sectors.[29] Given the importance of satellites to the national economy, the federal government's growing reliance on them, and the many threats that face them, failure to explicitly include satellites in the national approach to CIP leaves a critical aspect of the national infrastructure without focused attention.

Conclusions

Commercial satellite service providers use a combination of techniques to protect their systems from unauthorized use and disruption, including hardware on satellites, physical and logical controls at ground stations, and encryption of the links. Although this level of protection may be adequate for many government requirements, commercial satellite systems lack the security features used in national security satellites for protection against deliberate disruption and exploitation.

Federal agencies reduce the risk associated with their use of commercial satellites by controlling the satellite components within their responsibility—primarily the data links and communication ground stations. But the satellite service provider is typically responsible for most components—the satellite, TT&C links, and the satellite control ground stations. Because federal agencies rely on commercial satellite service providers for most security features, they also reduce their risk by having redundant capabilities in place. However, national satellite protection policy is limited because it pertains only to satellite systems that are used for national security information, addresses only techniques associated with the links, and does not have an enforcement mechanism. Recent initiatives by the Executive Branch have acknowledged these policy limitations, but we are not aware of specific actions taken to address them.

[29] U.S. General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach to Address Information Attacks*, GAO-02-474 (Washington, D.C.: July 15, 2002).

Satellites are not specifically identified as part of our nation's critical infrastructure protection approach, which relies heavily on public-private partnerships to secure our critical infrastructures. As a result, a national forum to gather and share information about industrywide vulnerabilities of the satellite industry does not exist, leaving a national critical infrastructure without focused attention.

Recommendations

We recommend that in pursuing the draft policy submitted to OMB for completion and the recommended review of U.S. space policies, the Director of OMB and the Assistant to the President for National Security Affairs review the scope and enforcement of existing security-related space policy and promote the appropriate revisions of existing policies and the development of new policies to ensure that federal agencies appropriately address the concerns involved with the use of commercial satellites, including the sensitivity of information, security techniques, and enforcement mechanisms.

Considering the importance of satellites to our national economy, the government's growing reliance on them, and the threats that face them, we recommend that the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the Special Advisor to the President for Cyberspace Security consider recognizing the satellite industry as either a new infrastructure or part of an existing infrastructure.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Deputy Assistant Secretary of Defense, Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (Space and Information Technology Programs), Department of Defense; the Chief of the Satellite Communications and Support Division, United States Space Command, Department of Defense; the Chief Financial Officer/Chief Administrative Officer, National Oceanic and Atmospheric Administration, Department of Commerce; and the Associate Deputy Administrator for Institutions, National Aeronautics and Space Administration. The Departments of Defense and Commerce and the National Aeronautics and Space Administration concurred with our findings and recommendations (see apps. II, III, and IV, respectively) and provided technical comments that have been incorporated in the report, as appropriate (some of these technical comments are reproduced in the appendixes).

We also received technical oral comments from officials from the Critical Infrastructure Assurance Office, Department of Commerce; Federal Aviation Administration, Department of Transportation; Office of Management and Budget; and United States Secret Service, Department of Treasury; in addition, we received written and oral technical comments from five participating private-sector entities. Comments from all these organizations have been incorporated into the report, as appropriate. We did not receive comments from the Special Advisor to the President for Cyberspace Security.

As we agreed with your staff, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to other interested congressional committees and the heads of the agencies discussed in this report, as well as the private-sector participants. The report will also be available on GAO's website at www.gao.gov.

If you have any questions about matters discussed in this report, please contact me at (202) 512-3317 or contact Dave Powner, Assistant Director, at (303) 572-7316. We can also be reached by E-mail at daceyr@gao.gov and pownerd@gao.gov, respectively. Contributors to this report include Barbara Collier, Michael Gilmore, Rahul Gupta, Kevin Secrest, Karl Seifert, Hai Tran, and Jim Weidner.

Sincerely yours,

Robert F. Dacey

Robert F. Dacey
Director, Information Security Issues

Objectives, Scope, and Methodology

Our objectives were to determine (1) what security techniques are available to protect satellite systems from unauthorized use, disruption, or damage; (2) how federal agencies reduce the risks associated with their use of commercial satellite systems; and (3) what federal critical infrastructure protection efforts are being undertaken to address satellite system security through improved government/private-sector cooperation. To accomplish these objectives, we reviewed technical documents, policy documents, and directives, and we interviewed pertinent officials from federal agencies and the private sector involved in manufacturing and operating satellites and providing satellite services.

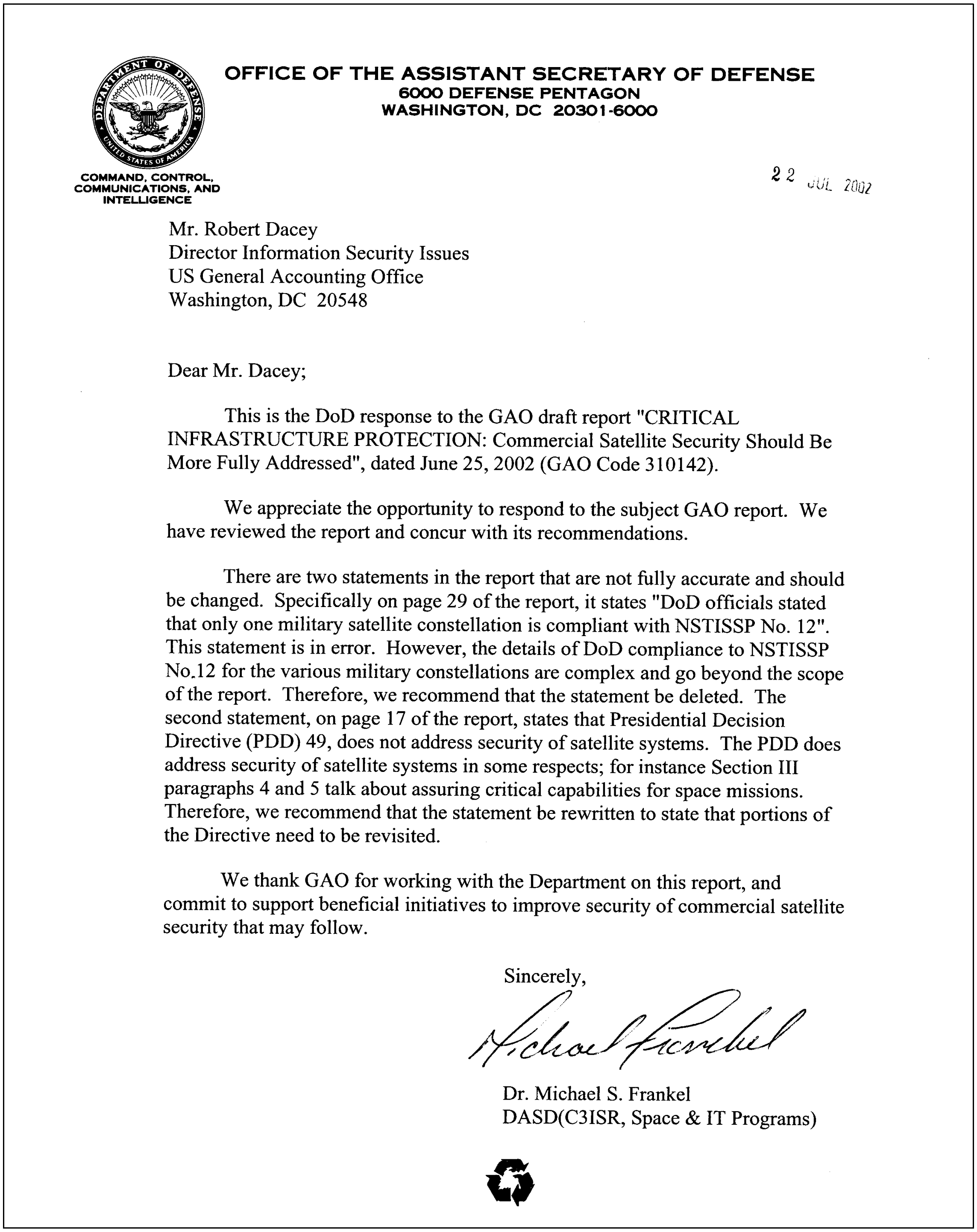
To determine what security techniques are available to protect satellite systems from unauthorized use, disruption, or damage, we reviewed technical documents and policy, such as NSTISSP No. 12 and various other sources, and we interviewed pertinent federal officials from the Department of Defense (DOD); the Federal Aviation Administration (FAA); the National Aeronautics and Space Administration (NASA), including the Goddard and Marshall Space Flight Centers; the National Oceanic and Atmospheric Administration (NOAA); the National Security Agency (NSA); and the Department of Treasury's United States Secret Service. The DOD organizations whose documentation we reviewed and whose officials we interviewed included the Air Force; the Army; the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; the Cheyenne Mountain Air Force Station; the Defense Information Systems Agency; the National Security Space Architect; the Navy; and the U.S. Space Command. In addition, we reviewed documentation and interviewed officials from private-sector organizations that manufacture and operate satellite systems, including Intelsat, Lockheed Martin, Loral Space & Communications, Ltd. (Loral Skynet and Loral Space Systems groups), Northrop Grumman TASC, the Satellite Industry Association, and W.L. Pritchard & Co., L.C. We identified these organizations through relevant literature searches, discussions with organizations, and discussions with GAO personnel familiar with the satellite industry. We did not develop an all-inclusive list of security techniques, but we attempted to establish the most commonly used of the security techniques available.

To determine how federal agencies reduce the risks associated with their use of commercial satellite systems, we identified and reviewed relevant federal policy, including National Security Telecommunications and Information Systems Security Committee policies and applicable federal agency policies, such as the FAA's *Information Systems Security Program Handbook*. We also reviewed documentation and interviewed federal officials from DOD, FAA, NASA, NSA, and NOAA. In addition, in meetings with commercial service providers holding government contracts, we discussed any special requirements placed on commercial service providers by federal agencies.

To determine what federal critical infrastructure protection (CIP) efforts were being undertaken to address satellite system security, we reviewed various orders, directives, and policies, such as Executive Order 13231 and PDD 63. In addition, we interviewed pertinent federal officials from the Critical Infrastructure Assurance Office, National Communications System/National Coordinating Center for Telecommunications, and National Telecommunications and Information Administration. Further, in interviews with commercial service providers, we discussed their involvement in national CIP-related activities.

We performed our work in Washington, D.C.; Bedminster, New Jersey; Colorado Springs, Colorado; and Palo Alto, California, from December 2001 through June 2002, in accordance with generally accepted government auditing standards. We did not evaluate the effectiveness of security techniques being used by federal agencies and the private sector, or of the techniques used by federal agencies to reduce the risks associated with their use of commercial satellite systems.

Comments from the Department of Defense



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

22 JUL 2002

Mr. Robert Dacey
Director Information Security Issues
US General Accounting Office
Washington, DC 20548

Dear Mr. Dacey;

This is the DoD response to the GAO draft report "CRITICAL INFRASTRUCTURE PROTECTION: Commercial Satellite Security Should Be More Fully Addressed", dated June 25, 2002 (GAO Code 310142).

We appreciate the opportunity to respond to the subject GAO report. We have reviewed the report and concur with its recommendations.

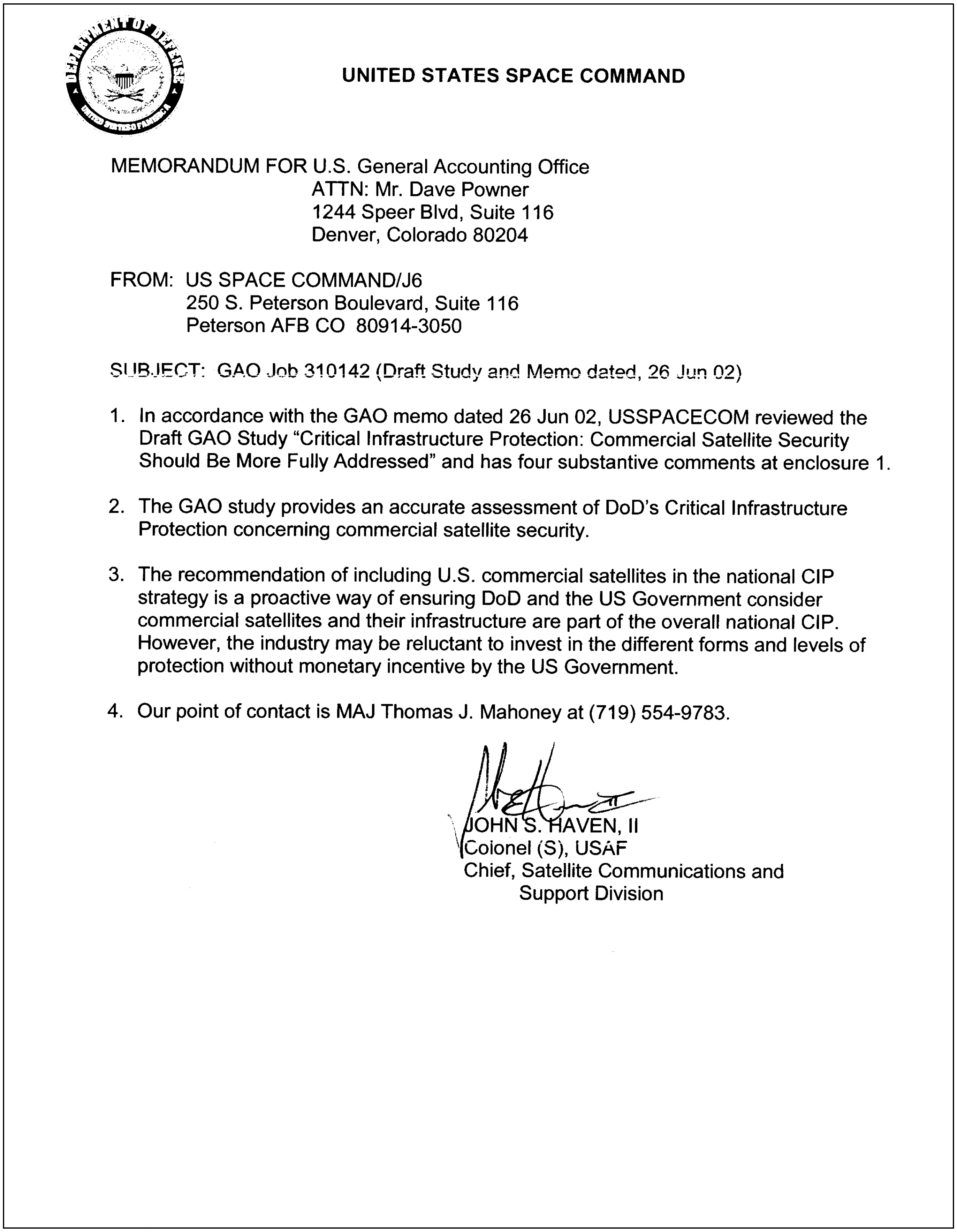
There are two statements in the report that are not fully accurate and should be changed. Specifically on page 29 of the report, it states "DoD officials stated that only one military satellite constellation is compliant with NSTISSP No. 12". This statement is in error. However, the details of DoD compliance to NSTISSP No.12 for the various military constellations are complex and go beyond the scope of the report. Therefore, we recommend that the statement be deleted. The second statement, on page 17 of the report, states that Presidential Decision Directive (PDD) 49, does not address security of satellite systems. The PDD does address security of satellite systems in some respects; for instance Section III paragraphs 4 and 5 talk about assuring critical capabilities for space missions. Therefore, we recommend that the statement be rewritten to state that portions of the Directive need to be revisited.

We thank GAO for working with the Department on this report, and commit to support beneficial initiatives to improve security of commercial satellite security that may follow.

Sincerely,

Michael Frankel

Dr. Michael S. Frankel
DASD(C3ISR, Space & IT Programs)



UNITED STATES SPACE COMMAND

MEMORANDUM FOR U.S. General Accounting Office
ATTN: Mr. Dave Powner
1244 Speer Blvd, Suite 116
Denver, Colorado 80204

FROM: US SPACE COMMAND/J6
250 S. Peterson Boulevard, Suite 116
Peterson AFB CO 80914-3050

SUBJECT: GAO Job 310142 (Draft Study and Memo dated, 26 Jun 02)

1. In accordance with the GAO memo dated 26 Jun 02, USSPACECOM reviewed the Draft GAO Study “Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed” and has four substantive comments at enclosure 1.

2. The GAO study provides an accurate assessment of DoD’s Critical Infrastructure Protection concerning commercial satellite security.

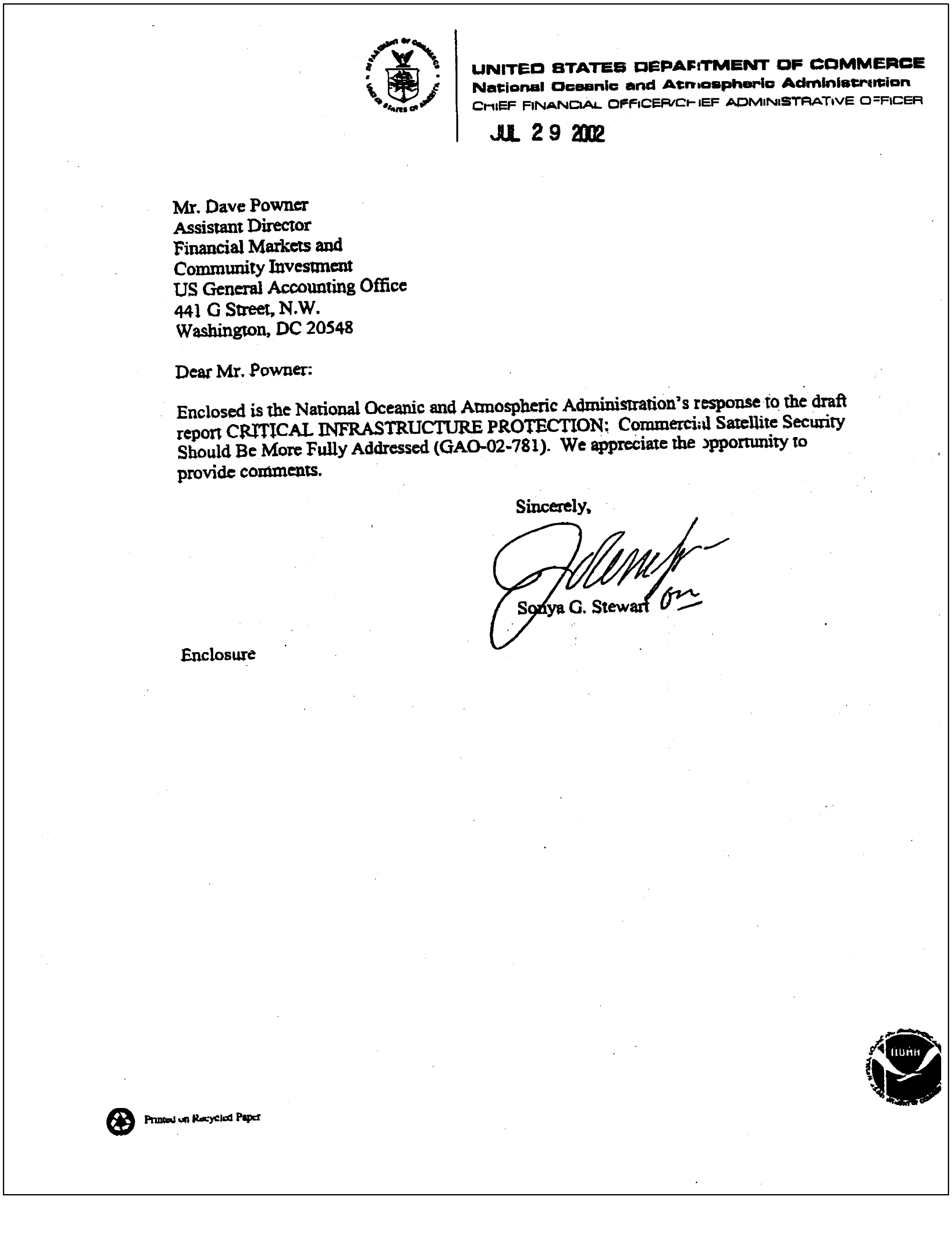
3. The recommendation of including U.S. commercial satellites in the national CIP strategy is a proactive way of ensuring DoD and the US Government consider commercial satellites and their infrastructure are part of the overall national CIP. However, the industry may be reluctant to invest in the different forms and levels of protection without monetary incentive by the US Government.

4. Our point of contact is MAJ Thomas J. Mahoney at (719) 554-9783.

JOHN S. HAVEN, II
Colonel (S), USAF
Chief, Satellite Communications and
Support Division

Appendix III

Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
CHIEF FINANCIAL OFFICER/CHIEF ADMINISTRATIVE OFFICER

JUL 29 2002

Mr. Dave Powner
Assistant Director
Financial Markets and
Community Investment
US General Accounting Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Powner:

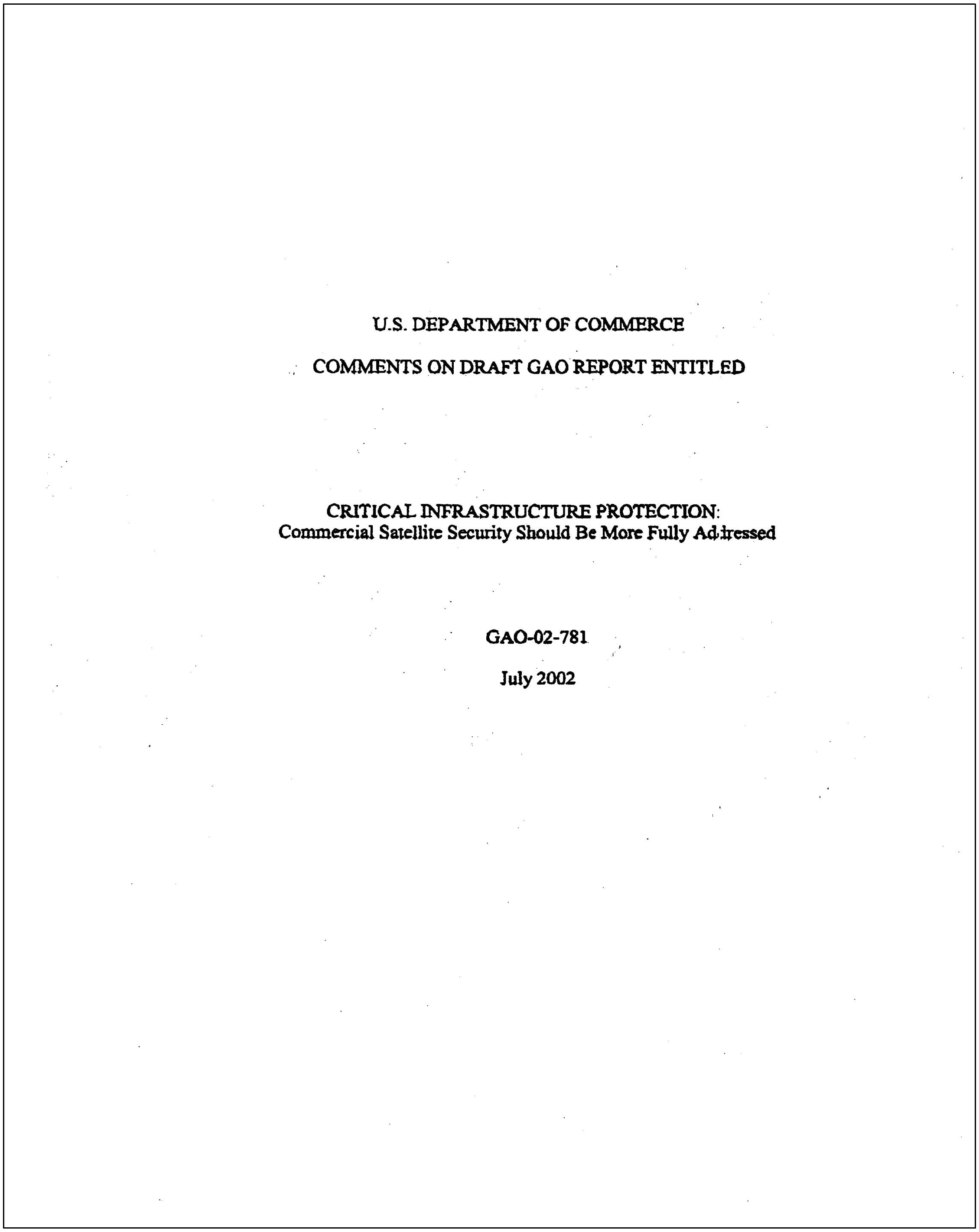
Enclosed is the National Oceanic and Atmospheric Administration's response to the draft report CRITICAL INFRASTRUCTURE PROTECTION: Commercial Satellite Security Should Be More Fully Addressed (GAO-02-781). We appreciate the opportunity to provide comments.

Sincerely,

Sonya G. Stewart

Enclosure

Printed on Recycled Paper



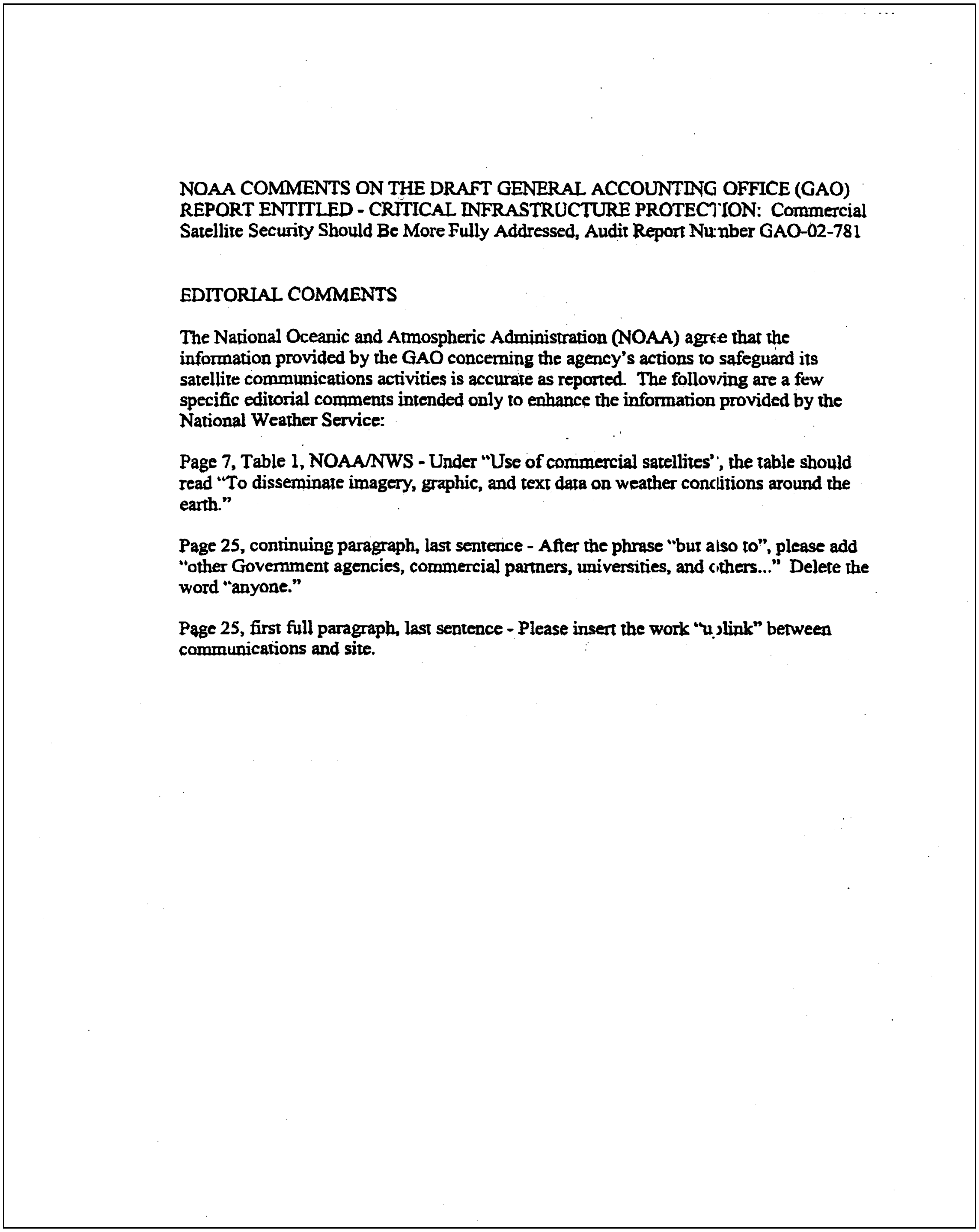
U.S. DEPARTMENT OF COMMERCE

COMMENTS ON DRAFT GAO REPORT ENTITLED

CRITICAL INFRASTRUCTURE PROTECTION:
Commercial Satellite Security Should Be More Fully Addressed

GAO-02-781

July 2002



NOAA COMMENTS ON THE DRAFT GENERAL ACCOUNTING OFFICE (GAO) REPORT ENTITLED - CRITICAL INFRASTRUCTURE PROTECTION: Commercial Satellite Security Should Be More Fully Addressed, Audit Report Number GAO-02-781

EDITORIAL COMMENTS

The National Oceanic and Atmospheric Administration (NOAA) agree that the information provided by the GAO concerning the agency's actions to safeguard its satellite communications activities is accurate as reported. The following are a few specific editorial comments intended only to enhance the information provided by the National Weather Service:

Now on p. 6.

Page 7, Table 1, NOAA/NWS - Under "Use of commercial satellites", the table should read "To disseminate imagery, graphic, and text data on weather conditions around the earth."

Now on p. 26.

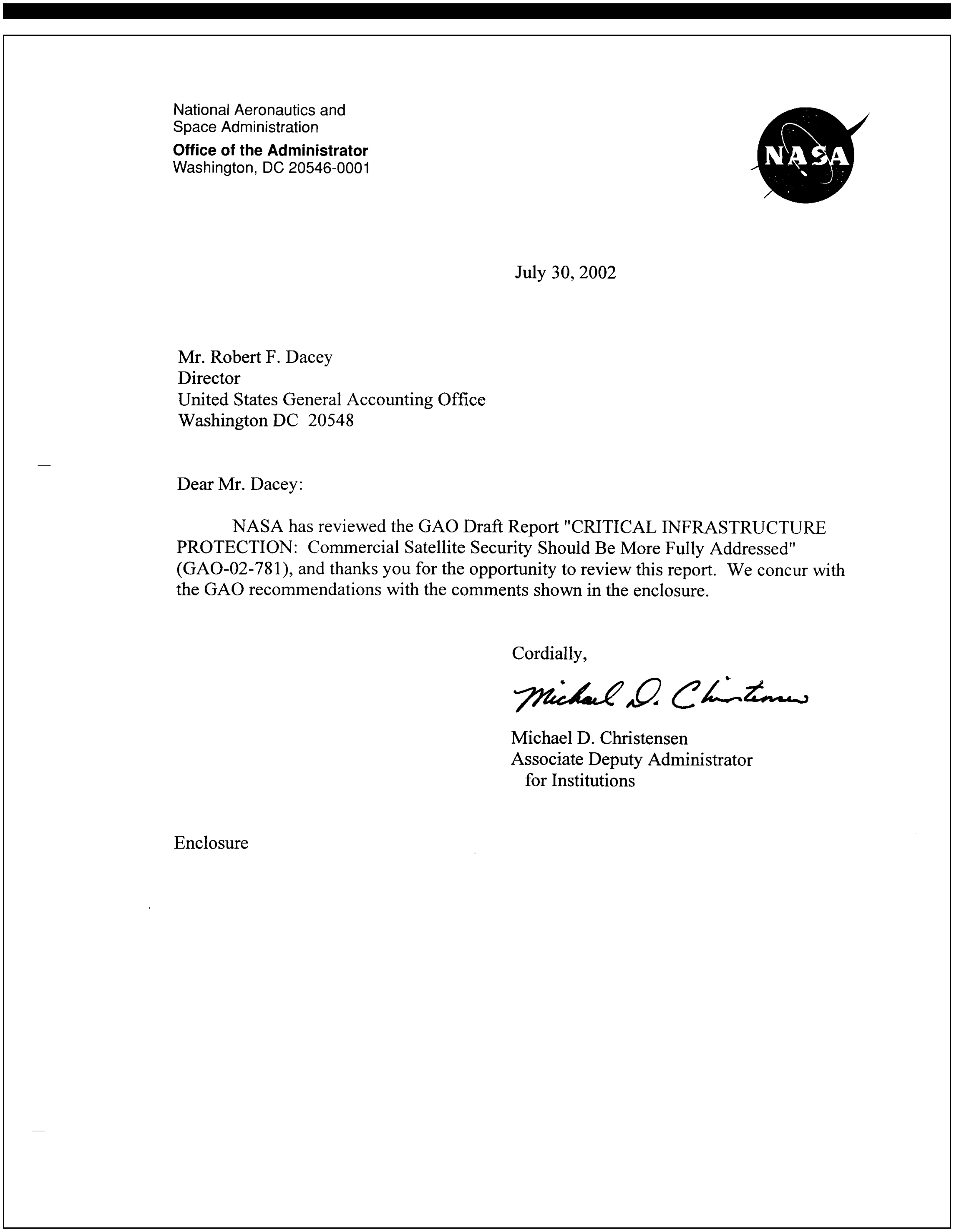
Page 25, continuing paragraph, last sentence - After the phrase "but also to", please add "other Government agencies, commercial partners, universities, and others..." Delete the word "anyone."

Now on p. 27.

Page 25, first full paragraph, last sentence - Please insert the work "uplink" between communications and site.

Appendix IV

Comments from the National Aeronautics and Space Administration



National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001

July 30, 2002

Mr. Robert F. Dacey
Director
United States General Accounting Office
Washington DC 20548

Dear Mr. Dacey:

NASA has reviewed the GAO Draft Report "CRITICAL INFRASTRUCTURE PROTECTION: Commercial Satellite Security Should Be More Fully Addressed" (GAO-02-781), and thanks you for the opportunity to review this report. We concur with the GAO recommendations with the comments shown in the enclosure.

Cordially,

Michael D. Christensen

Michael D. Christensen
Associate Deputy Administrator
for Institutions

Enclosure

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER

[redacted]