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.

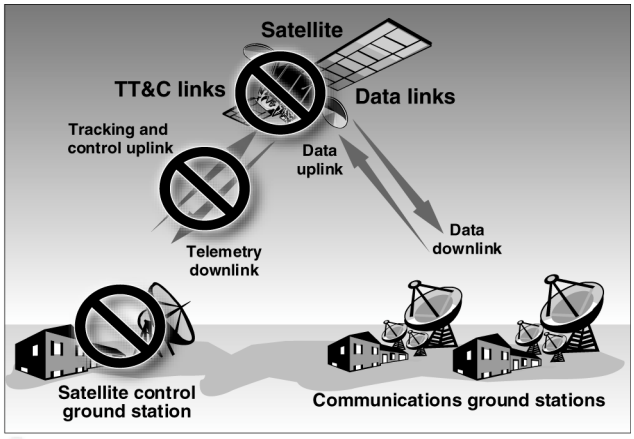
In commenting on a draft of this report, agencies included in our review concurred with our findings and recommendations. In addition, these agencies and private-sector entities provided technical comments, which were included in the report, as appropriate.

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 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.