



NATIONAL DEFENSE RESEARCH INSTITUTE

CHILDREN AND ADOLESCENTS
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE
U.S. NATIONAL SECURITY

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

[Jump down to document](#) ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore the [RAND National Defense Research Institute](#)

View [document details](#)

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of individual published, peer-reviewed documents or of a body of published work.



America's Publicly Available Geospatial Information

Does It Pose a Homeland Security Risk?

RAND RESEARCH AREAS
CHILDREN AND ADOLESCENTS
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
U.S. NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE

Federal agencies, state and local governments, industry, and other organizations produce, distribute, and use a wide variety of geospatial data and information. Much of this information—maps and nautical charts, aerial and satellite images, and detailed geographic information system databases—is used to help protect, operate, and manage a variety of vital sites in the United States, including critical infrastructure facilities and such key assets as national monuments, public gathering locations, and military installations. Other geospatial data provide a range of societal benefits, such as improving public safety and transportation access, advancing scientific understanding, and providing economic benefits.

In the wake of the September 11 attacks, the National Geospatial-Intelligence Agency (NGA) and the Department of the Interior's U.S. Geological Survey (USGS) asked the RAND Corporation's Intelligence Policy Center to assess how federal agencies' publicly accessible geospatial information could be exploited by possible attackers and to develop a framework that would help policymakers evaluate the nature of the potential risks of such information. Using a "demand" and "supply" approach, RAND researchers analyzed information that potential attackers would find most useful and assessed publicly available geospatial data, particularly from federal sources, concerning critical U.S. sites.

What Data Do Attackers Need?

Adversaries can take advantage of the relatively accessible nature of open societies, such as that of the United States, where a substantial number of critical infrastructure facilities (e.g., airports and tunnels) and other key assets are publicly accessible or can be directly observed from a distance. Terrorists and other potential attackers can choose opportunistically among the broad range of U.S. homeland locations, different strategic objectives, and a variety

Abstract

In the wake of the September 11 attacks, some U.S. federal agencies curtailed public access to various sources of geospatial information. While recognizing many public and private benefits of such information, officials were concerned that terrorists and other adversaries could exploit certain data (e.g., maps and overhead images) to attack key American assets and critical infrastructure. In the years since making those initial restrictions, however, policymakers have wrestled with how to distinguish between potentially sensitive information, which need not be restricted from the public, and truly sensitive information, to which public access must be restricted. To address this need, RAND developed an analytical process that U.S. officials can use to assess and filter publicly available geospatial information that has homeland security implications.

of attack modes. In general, attackers will possess two distinctive information needs: (1) what they need for *selecting a target* (i.e., which target and where is it located); and (2) what they need for *planning an attack* (i.e., what are the target's layout, vulnerabilities, security measures, etc.). Our analysis revealed that in targeting U.S. homeland locations, attackers have a broad range of choices about why, where, and how to attack. Adversaries, particularly terrorists, have substantial flexibility in choosing among potential targets and the information they use in planning and undertaking an attack. This permits them to adjust their target choices and information needs to satisfy their objectives.

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of individual published, peer-reviewed documents or of a body of published work.

Corporate Headquarters
1700 Main Street
P.O. Box 2138
Santa Monica, California
90407-2138
TEL 310.393.0411
FAX 310.393.4818

© RAND 2004

The RAND study concluded that although publicly accessible geospatial information has the potential to be generally helpful in selecting and locating a target, potential attackers, such as terrorists, are likely to need more reliable, more detailed, and more up-to-date information to plan and carry out a strike than is typically publicly accessible. There is abundant geospatial and nongeospatial information on U.S. critical sites that adversaries can obtain to select and locate targets. In comparison, planning an attack requires detailed and timely information, such as information on the target's internal features (e.g., control centers), potential vulnerabilities, and current security practices. Here, attackers confront a situation of relative "information scarcity" because such details are not normally made publicly accessible. Thus, attackers are more likely to turn to non-geospatial sources—including direct observation, academic textbooks, trade journals, and individuals familiar with the operations of a particular type of facility—to satisfy their information needs.

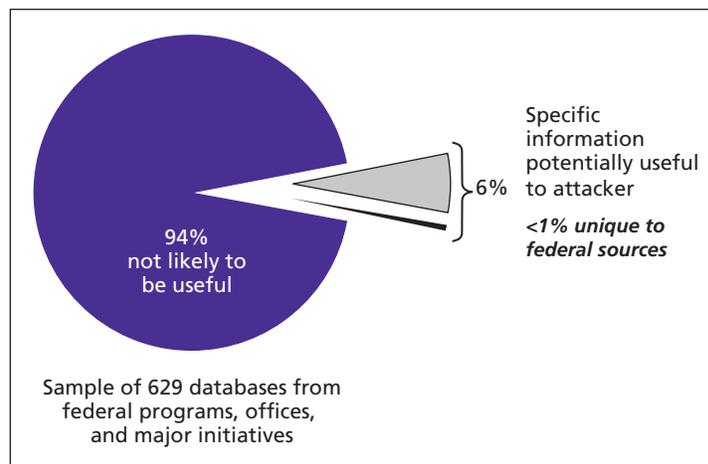
What Types of Geospatial Information Are Publicly Available?

What federal geospatial information is publicly available, and how significant is it to attackers' needs given the usefulness and uniqueness of the information? To answer these questions, the RAND research team:

- *Conducted a structured survey of publicly accessible federal geospatial data sources.* The survey identified and assessed publicly available geospatial information about critical sites at 465 federal data sources (i.e., federal programs, offices, and major initiatives), which involved searching more than 5,000 federal web sites.
- *Sampled geospatial datasets from these federal sources.* A selected sample of 629 federal datasets was identified for closer examination because they appeared most likely to contain geospatial information about U.S. critical sites.
- *Sampled alternative geospatial information sources.* A sample of more than 300 nonfederal sources (e.g., private, state and local government, academic, nongovernmental, and foreign geospatial data sources), involving a search of over 2,000 web sites, was assessed to determine the availability of nonfederal sources of geospatial information.

The figure depicts RAND's findings from examining these samples. Fewer than 6 percent of the 629 federal geospatial information datasets examined appeared as though they could be useful to meeting a potential attacker's information needs. Furthermore, the study found no publicly available federal geospatial datasets that might be considered critical to meeting the attacker's information needs (i.e., those that the attacker could not perform the attack without). Additionally, most publicly accessible federal geospatial information appears unlikely to provide significant (i.e., useful and unique) information for satisfying attackers' information needs (i.e., less than 1 percent of the 629 federal datasets examined appeared both potentially useful and unique). Moreover, since the September 11 attacks these *useful and unique* information sources are no longer being made public by federal agencies. In many cases, diverse alternative information sources exist. A review of nonfederal information

Less than 1 Percent of Federal Datasets Appear Potentially Useful and Unique



sources suggests that identical, similar, or more useful data about critical U.S. sites are available from industry, academic institutions, nongovernmental organizations, state and local governments, foreign sources, and even private citizens.

The RAND study suggests that sensitive geospatial information that is publicly available is not distributed widely and may be scarce. However, the RAND findings *do not* rule out the possibility that potential attackers could exploit existing or future geospatial information that is publicly accessible. Thus, U.S. policymakers need an analytical process for assessing the homeland security implications of geospatial information.

Importance of Weighing Societal Benefits and Costs

Any decisions to restrict public access to all or part of a particular geospatial dataset need to consider whether the expected homeland security benefits outweigh the likely societal costs. Although making such judgments is neither easy nor exact, decisionmakers have a responsibility to consider the societal costs of restricting public access, even if such costs can only be roughly gauged at best.

Federal geospatial information provides many benefits to a wide range of users, including other federal agencies, state and local governments, private firms, nongovernmental organizations, and community groups. Furthermore, people who work, recreate, or live near a critical site need the geospatial information about the site to access or to avoid the location when conducting their activities. The boating, fishing, and oil and gas industries, for example, need accurate nautical charts. Emergency responders and planners need up-to-date geospatial data to provide services in the event of a natural disaster, accident, or terrorist incident. Public availability of such geospatial information is often required by federal, state, or local laws. In addition, broad access to geospatial data and information is integral to increasing productivity, reducing private- and public-sector costs of doing business, facilitating knowledge sharing, and enhancing U.S. international competitiveness.

Although the societal benefits of particular geospatial information are often difficult to quantify, decisionmakers who are responsible for determining what information should be publicly accessible should seek to identify the range of potential information users and assess the opportunity costs that limiting access would impose on users.

An Initial Framework for Analysis

The study recommends that the federal government should be proactive in making the process of reviewing publicly available geospatial information more coherent and consistent among a wide range of federal agencies and relevant nonfederal organizations. RAND researchers developed an initial framework that policymakers can use to assess the homeland security implications of publicly available geospatial information. The framework incorporates three distinct filters as shown in the table.

Such an analytical process, if used widely, can assist decisionmakers by providing a structured and consistent approach to identifying sensitive geospatial information and an explicit methodology to justify and explain decisions that affect public access to geospatial information.

Need for Leadership

For the longer term, the federal government needs a more comprehensive model for addressing the security implications of geospatial information. This model should provide a means to match desired protection levels with threats, identify relative protection profiles to defeat these threats, and set forth a structured set of evaluation criteria. Facilities and installations, in turn, could be associated with those protection levels based on their particular needs.

The federal government needs to take a lead role in this effort. Not only do federal agency staffs need practical guidance, but non-federal organizations (e.g., state and local governments and private firms operating critical infrastructure facilities) also have a strong need for federal government insights and guidance. As agencies with relevant expertise, NGA and USGS should play a substantial part in helping the Department of Homeland Security, the Office of Management and Budget, and other organizations develop policy guidelines for identifying sensitive geospatial information. ■

Initial Framework for Assessing the Homeland Security Sensitivity of Publicly Available Geospatial Information

Filter	Key Questions
Usefulness	Is information useful for target selection or location purposes? Is information useful for attack planning purposes?
Uniqueness	Is information readily available from other geospatial information sources? Is information available from direct observation or other nongeospatial information types?
Societal benefits/costs	What are the expected security benefits of restricting public access to this geospatial information? What are the expected societal costs of restricting public access to this geospatial information?

This research brief describes work done for the RAND National Defense Research Institute documented in *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information*, by John C. Baker, Beth E. Lachman, David R. Frelinger, Kevin M. O'Connell, Alexander C. Hou, Michael S. Tseng, David Orletsky, and Charles Yost, MG-142-NGA (available at www.rand.org/publications/MG/MG142), 2004, 231 pp., \$24.00, ISBN: 0-8330-3547-9. MG-142 is also available from RAND Distribution Services (phone: 310.451.7002; toll free: 877.584.8642; or email: order@rand.org). The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RAND Offices Santa Monica • Washington • Pittsburgh • New York • Doha • Leiden • Berlin • Cambridge