This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Mapping the Risks

Assessing the Homeland Security Implications of Publicly Available Geospatial Information

JOHN C. BAKER, BETH E. LACHMAN, DAVID R. FRELINGER, KEVIN M. O'CONNELL, ALEXANDER C. HOU, MICHAEL S. TSENG, DAVID ORLETSKY, CHARLES YOST

Prepared for the National Geospatial-Intelligence Agency

NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was prepared for the National Geospatial-Intelligence Agency. The research was conducted in the RAND National Defense Research Institute, a federally funded research and development center supported by the Office of the Secretary of Defense, the Joint Staff, the unified commands, and the defense agencies under Contract DASW01-01-C-0004.

Library of Congress Cataloging-in-Publication Data

Mapping the risks : assessing homeland security implications of publicly available geospatial information / John C. Baker ... [et al.].
p. cm.
"MG-142."
Includes bibliographical references.
ISBN 0-8330-3547-9 (pbk. : alk. paper)
1. Civil defense—United States. 2. Geographic information systems—Defense measures—United States. I. Baker, John C., 1949–

UA927.M26 2004
363.34'7'0285—dc22

2003027797

Published 2004 by the RAND Corporation
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

In the wake of the September 11, 2001 terrorist attacks, U.S. officials have instituted information protection policies aimed at bolstering homeland security. These policies aim to minimize the opportunities of potential attackers exploiting publicly available information they might obtain from federal sources in planning attacks against U.S. homeland locations.

Of particular concern to U.S. officials are the federal sources of geospatial information. Geospatial data and information are useful for identifying various geographical features of U.S. locations and facilities, as well as characterizing their important attributes. Although federal agencies produce and publicly disseminate such information for a wide range of beneficial purposes, the risk also exists that some types of geospatial information could be exploited by terrorists. Federal agencies thus face a challenge in deciding which types of geospatial information should be publicly accessible, as well as whether and how to restrict new sensitive information as it becomes available.

Study Purpose and Approach

This study frames the analytical issues associated with assessing whether and how geospatial data and information that is publicly available from U.S. federal agencies can be exploited by potential attackers, including terrorists, for attacking U.S. critical infrastructure and other key homeland locations. The results of our analysis yield

insights that can assist federal and other decisionmakers by highlighting key factors they should consider in addressing this issue. The study also offers an analytical process that can serve as an initial framework for assessing publicly available geospatial information in order to understand its homeland security implications.

The Need for a Framework to Support Decisionmaking

Decisionmakers are faced with the task of deciding whether publicly accessible geospatial information poses a risk to protecting critical infrastructure and, if so, whether to restrict public access to the information. After September 11, officials had to make decisions about restricting such access under conditions of time pressures and without much top-level guidance. However, even under the best circumstances, assessing what information is potentially sensitive and what warrants restriction is not easy. An analytical process can assist decisionmakers by

- providing a structured and consistent approach to identifying sensitive geospatial information
- ensuring that all relevant factors are weighed
- providing an explicit methodology and rationale to justify and explain the decision.

A basic premise of our analysis is, therefore, that sound decisions about the security benefits of restricting a particular piece or type of geospatial information depend on considering their homeland security implications in broader contexts. These implications are the following:

- *Usefulness*: the potential usefulness of geospatial information for planning attacks on critical U.S. sites. Attackers require particular kinds of information to identify targets and plan attacks.
- *Uniqueness*: the uniqueness of federal geospatial information sources. If alternative sources of the same information are readily available, the net security benefits of restricting access to the information may be minimal or nonexistent.

- *Benefits and Costs*: the expected societal benefits and costs of restricting the information. The chief benefit of restricting public access to geospatial information should be to improve U.S. homeland security against an attack. However, any expected benefits also must be weighed against expected societal costs, which are likely to exist because of the many important public- and private-sector uses.

A "Supply" and "Demand" Approach to Developing the Framework

To help decisionmakers think about these broader contexts, we conducted analysis intended to derive a framework for factoring these considerations into decisions about whether to restrict public access to geospatial information. We used a two-pronged approach to formulate this framework:

- We assessed attackers' potential information needs—the "demand."
- We thoroughly examined federal sources of publicly available geospatial information—the "supply"—and reviewed a sampling of alternative nonfederal sources that provide similar types of information.

Scope of the Analysis

We defined geospatial information broadly, including geospatial data and information that exist in a variety of forms and are accessible through various media and sources. The forms range from raw geospatial data (e.g., latitude and longitude coordinates, maps and nautical charts, aerial and satellite images, textual geospatial descriptions) to relatively sophisticated geospatial datasets (e.g., detailed, high-accuracy geographic information system [GIS] databases).

Because of tasking and time constraints, this study does not address the following related topics, which fall outside the scope of this report:

- information without a direct or indirect geospatial characteristic

- data and information that are classified or withheld from the public under the Freedom of Information Act for homeland security or national security purposes
- new and potentially sensitive information that might be created via the integration of data from diverse sources
- nonsecurity rationales for restricting public access to data.

Demand: Assessing Attackers' Information Requirements

Methodology

To gain insights on the key information needs of potential attackers on the U.S. homeland, we undertook an analysis involving a series of postulated attacks on a spectrum of critical infrastructure, military targets, and cultural and social targets. The rationales for the attacks were derived from plausible attacker motivations, historic preferences for attack modalities by a number of real-world organizations, opportunities associated with some weapon systems that are becoming more widespread, and the use of modern techniques and tools for targeting (e.g., remote sensing, geospatial information systems, GPS [Global Positioning System], range finders). These attacks were quantitatively evaluated in terms of the likely damage they would cause. The results of these assessments informed our analysis and the findings presented in this report.

Analysis

Attackers can take advantage of the relatively accessible nature of the United States, where a substantial number of critical infrastructure facilities (e.g., airports, tunnels) and other key locations are publicly accessible or can be directly observed from a distance. Attackers can choose opportunistically among a broad range of U.S. homeland locations, different strategic objectives and related targeting objectives, and a variety of attack modes ranging from ground attacks with explosives to standoff weapon systems and area weapons (e.g., chemical, radiological). Attackers also have flexibility in both choosing

among potential targets and the information they use in planning and undertaking an attack.

The geospatial information requirements of potential attackers fall largely into two categories:

- information for *selecting a target* (i.e., Which target?, Where is it located?)
- information for *planning the attack* (i.e., What is the target's layout, vulnerabilities, security measures, etc.?).

The first type of information assists attackers in identifying a potential target and determining its general location. The attacker benefits from today's "information abundance"—that is, both geospatial and nongeospatial information is widely available from many sources. In comparison, planning an assault requires detailed and timely information for the attacker to have confidence in executing a successful operation against a given target. This planning can require information on the internal features of the selected target site (e.g., control centers, power sources), the potential vulnerabilities of the facility, and a facility's current security practices. In these cases, attackers confront a situation of relative "information scarcity" in terms of what is publicly available.

Findings

In terms of the information demands of potential attackers, our key findings are as follows:

- **Attackers have substantial flexibility in fulfilling their information needs for attacking U.S. homeland locations.** In principle, this flexibility includes a broad range of choices about why, where, and how attacks will be made. This has important implications for the types of information that attackers need and can acquire for target selection and attack planning. Our assessment of attackers' information requirements suggests that, given this degree of flexibility, publicly accessible geospatial information is probably not the first choice for fulfilling these needs. Publicly

accessible geospatial information has the potential to be somewhat useful for helping with selecting a target and determining its location. However, potential attackers, such as terrorist groups or hostile governments, are more likely to desire more reliable and timely information, which is often obtainable via other means, such as through direct access or observation. In addition, many types of attacks, such as those by ground parties, are likely to require detailed information for attack planning purposes (depending on the target type and mode of attack). This type of information, which mostly comes from such nongeospatial sources as engineering textbooks or human expertise on the operations of a particular type of industrial complex, is essential for attackers to have a high confidence in their plan.

- **Opportunistic attackers, such as terrorists, usually possess the advantage of having access to diverse sources for meeting their mission-critical information needs, as well as the freedom to adjust the attack to meet the amount of information available.** An important distinction exists between what is critical information for the attacker (i.e., information with which the terrorist could not perform the attack), what is useful (but was not necessary to undertake the attack), and what is other nonessential information. Lacking critical information on a target could in theory discourage an attacker from proceeding with a given attack. In practice, however, an opportunistic attacker, such as a terrorist group, can exploit diverse information sources (ranging from direct observation to publicly available geospatial information) to meet critical information needs, while the defender faces the challenge of denying the attacker access to all relevant sources of information. The attacker can also change the mode of attack to better match the amount and type of information available. For example, if information is unavailable to support a direct assault on a target, standoff attacks on a different part of the complex or attacks outside the most heavily defended area producing the same or similar effect could be substituted. Similarly, if detailed plans are unavailable on a target to facilitate the

use of precisely placed munitions, weapons with a larger area of impact or different phenomenology might be used to generate the desired impact.

Supply: Assessing the Significance of Publicly Available Geospatial Information

Methodology

Our supply analysis focused on two key questions: (1) What federal geospatial information is publicly available? and (2) How significant is it to attackers' needs given the usefulness and uniqueness of the information? Namely, significance is a combined measure of *usefulness* and *uniqueness*. For this analysis, we identified and examined geospatial data using three main methods:

- **Identifying federal geospatial information sources.** We conducted a structured survey to identify and assess publicly available geospatial information about critical sites at 465 federal data sources. This systematic search involved several person-months of effort and the searching of more than 5,000 federal Web sites to identify and examine federal activities that provide publicly accessible geospatial information. We supplemented this search with selected interviews and hard-copy document reviews.
- **Sampling of geospatial datasets from federal sources.** Once federal sources for publicly available geospatial information were identified, we examined particular sources in more detail to determine whether they contained information that might be relevant to a potential attacker's information needs. Of these sources, we identified a selected sample of 629 federal datasets[1]

[1] A dataset refers to a single data file, Web page, or document containing geospatial information, while a database refers to an organized collection of datasets—that is, a set of data files. An example of a database is the National Atlas of the United States (see www.

that looked like they might contain some type of geospatially oriented critical-site information. We chose this sample by identifying datasets that appeared most likely to contain sensitive geospatial information about U.S. critical sites.

- **A sampling of alternative geospatial information sources.** Since our primary focus was on federal sources, we conducted a similar, though less thorough, systematic survey to identify and sample nonfederal sources (e.g., private-sector organizations, state and local governments, academic institutions, nongovernmental organizations [NGOs], foreign sources). This involved searching more than 2,000 nonfederal Web sites to identify and examine nonfederal activities that provide publicly accessible geospatial information and the identification of a sample of more than 300 nonfederal alternative sources. This search was not meant to be exhaustive; rather, we sought to selectively sample alternatives to understand the range of other sources and identify and examine ones that most likely contained sensitive geospatial information about U.S. critical sites.

Analysis

To assess the significance of federal geospatial information to an attacker's information needs, we performed three steps for our sample of 629 federal datasets:

1. Using our "demand" analysis, we assessed and ranked the usefulness of each federal geospatial dataset to the attacker's information needs.
2. We assessed and ranked the availability of the same or similar geospatial information from alternative sources to determine the uniqueness of each federal geospatial dataset.
3. We assessed and ranked the significance of the federal geospatial information by combining the measures of usefulness and uniqueness. This combination is important because a dataset

---

nationalatlas.gov), which contains population, water, species, land cover, boundary files, and many other datasets.

that is both useful and unique would be considered more sensitive information and parts of the dataset may warrant restriction.

Findings

Our findings concerning the supply of publicly available geospatial information from federal agencies and other sources are as follows:

- **Our federal geospatial information survey found that publicly available geospatial information is spread across a wide range of federal government agencies and offices.** Many different agencies serve as major distributors of publicly available geospatial information. We identified 465 programs, offices, or major initiatives at 30 different federal agencies and departments that make various types of geospatial information publicly accessible.
- **Our analysis found that very few of the publicly accessible federal geospatial sources appear useful to meeting a potential attacker's information needs.** Fewer than 6 percent of the 629 federal geospatial information datasets we examined appeared as though they could be useful to a potential attacker. Further, we found no publicly available federal geospatial datasets that we considered critical to meeting the attacker's information needs (i.e., those that the attacker could not perform the attack without).
- **Our analysis suggests that most publicly accessible federal geospatial information is unlikely to provide significant (i.e., useful and unique) information for satisfying attackers' information needs.** Fewer than 1 percent of the 629 federal datasets we examined appeared both potentially useful and unique. Moreover, since the September 11 attacks, these information sources are no longer being made public by federal agencies.[2] However, we cannot conclude that *publicly accessible* federal geospatial

[2] These federal geospatial sources have either been completely withdrawn from public access on the World Wide Web, or their agencies have implemented password protection to control access.

information provides no special benefit to the attacker. Neither can we conclude that it would benefit the attacker. Our sample suggests that the information, if it exists, is not distributed widely and may be scarce.

- **In many cases, diverse alternative geospatial and nongeospatial information sources exist for meeting the information needs of potential attackers.** In our sampling of more than 300 publicly available nonfederal geospatial information alternative sources, we found that the same, similar, or more useful geospatial information on U.S. critical sites is available from a diverse set of nonfederal sources. These sources include industry and commercial businesses, academic institutions, NGOs, state and local governments, international sources, and even private citizens who publish relevant materials on the World Wide Web. Some geospatial data and information that these nonfederal sources distribute are derived from federal sources that are publicly accessible. Similarly, these nonfederal organizations are increasingly becoming sources of geospatial data and information for various federal agencies (see Chapter Three for additional discussion). In addition, relevant information is often obtainable via direct access or direct observation of the U.S. critical site.

Framework to Support Decisionmaking

Our demand and supply analysis, along with a corresponding analysis of the broader societal benefits and costs of public access to geospatial information, identified key factors relevant to assessing the homeland security implications of geospatial information. Drawing on these insights, this study suggests that a useful, first-step framework for assessing geospatial information should incorporate at least three key factors: the usefulness of the information to an attacker, the uniqueness of the information, and the societal benefits and costs of restricting public access to a particular geospatial information source (see Table S.1). These factors, or "filters," offer decisionmakers and

Table S.1
Top-Level Framework for Analysis of the Homeland Security Sensitivity of Geospatial Data and Information Sources

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

analysts a more structured method for assessing the sensitivity of geospatial information. For individual geospatial datasets, federal decisionmakers could use this framework to help assess whether to restrict access to part or all of the database. In addition, this framework is relevant to all distributors of geospatial information, including industry, state and local governments, NGOs, and academic institutions. How would decisionmakers apply this framework? Decisionmakers would ask pertinent questions for each filter. The filtering questions would then be applied sequentially. To begin, decisionmakers would evaluate a particular piece of geospatial information through the first filter by asking whether the information could be useful for either the target selection or location, or the attack planning purposes of a potential attacker. Next, the information would be subject to the second filter, which focuses on assessing whether the information is relatively unique—that is, whether the geospatial information in question could be readily obtained by potential attackers using other sources. These sources could be either nonfederal geospatial (e.g., private-sector or state or local sources) or from direct access to or observation

of a potential target without incurring significant risks of being caught. Geospatial information that is both useful to the attacker and not readily available from alternative sources should be subjected to the third filter, which considers the likely societal benefits and costs of restricting public access to this potentially sensitive information. For example, is public access required for local public safety needs?

Once decisionmakers proceed through the framework and determine that a particular piece of information may need to be restricted, they face the question of how to limit public access. This determination will depend on additional considerations because a variety of options as well as precedents exist for restricting public access to federal geospatial information sources. In addition, since our analysis showed that geospatial information is spread across a diverse range of federal and nonfederal sources, controlling any particular type of geospatial data could be challenging. If the objective were to enhance security, imposing information controls would be complicated by the likelihood in most cases that potential attackers could exploit diverse sources of geospatial and other types of relevant information.

Ultimately, these decisions, particularly those concerning the societal costs of restricting access, are neither easy nor exact. Evaluations of the benefits of geospatial information being publicly accessible are not readily available. Unfortunately, comprehensive or in-depth studies assessing the specific value of keeping such information publicly accessible have not yet been conducted and accepted.

Nonetheless, our framework provides a useful step in developing a consistent and uniform analytical process for federal agency decisionmakers to identify key considerations in making decisions on restricting public access to geospatial information.

Broader Implications

In addition to the specific findings, several broader implications emerged from our analysis. The following observations speak to broader aspects on the nature of geospatial information sources, the

usefulness of geospatial information for potential attackers on U.S. homeland locations, and the role that the federal government could play in providing guidance to agencies about whether and how to restrict such information:

The ability of potential attackers to exploit publicly available geospatial information significantly varies with the type of information needed. With some important exceptions, the geospatial information needed for identifying and locating potential targets is widely accessible. In comparison, detailed and up-to-date information required for attack planning against a particular target is much less readily available from publicly available sources. A diverse range of geospatial data and information sources exist that could be exploited by attackers trying to meet their target identification information needs. Given the ready availability of alternative data sources, restricting public access to such geospatial information is unlikely to be a major impediment for attackers in gaining the needed information for identifying and locating their desired targets in the United States. The key exception to this general expectation is any type of geospatial information that reveals the location of vulnerabilities in the critical infrastructure that are not obvious or widely known, such as a particular choke point in a major power grid or telecommunications network. Compared with the ready availability of information that permits target identification and location, useful attack planning information for a particular critical infrastructure facility is much more difficult to find in publicly available sources. Given this condition of "information scarcity," any publicly available sources providing this type of detailed and timely information (e.g., internal facility equipment layout details, specifics on the security perimeter) should be more closely examined concerning their potential sensitivity for homeland security.

Our results do not rule out the possibility that federal publicly available geospatial information could be exploited by potential attackers, including the possibility that discrete pieces of such information could be aggregated by the attacker with the aim of achieving greater targeting value than is apparent when the information is viewed separately. However, these pieces of information

should be identified in the context of how they might be specifically used by potential attackers. In addition, because widely available nonfederal sources often exist with similar geospatial information, alternative sources need to be assessed. Therefore, an analytical process is needed to evaluate individual geospatial datasets concerning their potential risks for protecting U.S. critical sites and whether restricting public access to certain parts of, or all of, the datasets would enhance homeland security.

Decisions about whether and how to restrict geospatial information would benefit from applying an analytic framework to help assess the sensitivity of a piece of geospatial information being publicly available and the security benefits and societal costs of restricting public access. The analytical approach presented in this study integrates three distinct filters—usefulness, uniqueness, and societal benefits and costs—as a first-step framework for decisionmakers to help evaluate whether a geospatial source is potentially sensitive and whether public access should be curtailed in some way. An explicit framework for analysis offers decisionmakers several benefits, including a way of making more structured and uniform decisions on whether and how to restrict public access to geospatial information and a better way of explaining the basis for such decisions to others.

Assessing the societal benefits and costs of restricting public access to geospatial information sources is not straightforward. Along with assessing the expected security benefits of restricting public access to certain types of information, our analytical framework seeks to weigh the societal costs of limiting public access. Most publicly available geospatial information addresses particular public and private needs for such information, including public safety, health, and economic development. For example, people working, recreating, or living near a critical site (e.g., chemical plants, gas pipelines) need geospatial information about a site to make decisions about accessing or avoiding the location when conducting their activities. However, gauging the costs of restricting public access is complicated by the limitations in existing methodologies for quantifying the specific benefits and costs of public access to geospatial information. Key decisions on restricting public access on geospatial information would

be best made in a process that allows senior U.S. decisionmakers to make impartial judgments on the relative merits of these complex choices apart from the competing interests of stakeholders.

The federal government has a unique role in providing geospatial guidance to federal agencies, as well as insights on information sensitivity for nonfederal organizations. We conclude that civilian and military agencies have a growing need for well-founded and consistent guidelines for identifying geospatial data and information that could have homeland security implications. In addition, nonfederal organizations also need similar guidance in making decisions on information protection policies involving geospatial data and information.

General Recommendations

This report presents four general recommendations:

The federal government should play a proactive role in bringing greater coherence and consistency to assessing the homeland security implications of publicly available geospatial information. Federal agency staffs need practical guidance to assist them in framing choices about whether to place new restrictions on public access to parts of their geospatial information or to modify the restrictions imposed after the September 11 attacks.

An analytical process should be used by federal agencies and other organizations to assess the potential homeland security sensitivity of specific pieces of publicly available geospatial information and whether restricting access would enhance security. The analytical framework presented earlier is a useful first step that is immediately available for helping federal decisionmakers make sound and consistent assessments on whether and how to restrict public access to geospatial information for the purposes of enhancing U.S. homeland security. We also believe that this framework can be useful for any decisionmaker, not just federal ones, faced with the same type of determination.

For the longer term, the federal government should develop a more comprehensive model for addressing the security of geospatial information. A more formal and comprehensive model should be developed to provide a means of associating desired protection levels relative to the type of threats, relative protection profiles to defeat these threats, and a structured set of evaluation criteria. Facilities and installations could be, in turn, associated with those protection levels based on the particular needs of individual facilities and installations. Based on a process that integrates diverse expertise, a more comprehensive and formal model would provide public- and private-sector decisionmakers with a consistent level of protection for a wide variety of different types of facilities. It would also focus discussion away from how the data are to be protected to the more difficult question of what level of protection is appropriate for a given facility or installation.

In addition, the federal government should increase the awareness of the public and private sectors concerning the potential sensitivity of geospatial information. The federal government is uniquely positioned to generate and disseminate insights on the potential homeland security sensitivity of various types of geospatial data and information produced or distributed by a wide range of nonfederal organizations, including state and local governments, NGOs, and private-sector firms involved in geospatial activities or that operate critical infrastructure facilities.

Agency-Specific Recommendations

We expect that the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB) will serve as lead policymaking agencies in formulating policy for U.S. federal agencies dealing with the homeland security implications of publicly available geospatial information. Similarly, as the lead homeland defense command operation, U.S. Northern Command (NORTHCOM) is likely to play a major role in providing guidance to a wide range of

military decisionmakers concerned with force protection at U.S. installations.

However, as primary government agencies that produce and distribute geospatial data and information, the National Geospatial-Intelligence Agency (NGA, formerly the National Imagery and Mapping Agency) and the U.S. Geological Survey (USGS) of the Department of the Interior (DOI) could play a substantial role in applying their special expertise to help other organizations in identifying sensitive geospatial information. Both NGA and USGS possess unique capabilities and expertise relevant to helping the federal government develop guidelines for identifying sensitive geospatial information.

NGA should take advantage of its special expertise in geospatial intelligence to give other organizations a general sense of how various types of geospatial data and information could be exploited by potential adversaries for attacking U.S. critical infrastructure facilities and other key locations, including military installations. Specifically, NGA should leverage its expertise in such key areas as processing experience, military targeting, data integration, and knowledge of foreign geospatial information policies and practices.

Similarly, USGS can offer insights based on its relevant expertise in science-based applications and its strong sense of the breadth of domestic and international sources of publicly available geospatial information. USGS also has a good appreciation of the range of public and private stakeholders likely to be affected by any changes in public access to these types of data and information.

This report provides a framework for analysis that is relevant to decisionmakers who have responsibility for identifying and assessing geospatial information with homeland security implications. We conclude that there is a strong need for coherent and consistent guidelines to help federal agencies determine whether a specific piece of geospatial data and information is potentially sensitive and, if so, whether it should be considered for partial or complete restrictions concerning public access. Conversely, well-founded guidelines can also serve the public interest by giving decisionmakers a credible basis for modifying or dropping restrictions to geospatial sources in cases in

which circumstances warrant such changes. In both instances, such guidelines should be shared with nonfederal public- and private-sector organizations that have similar responsibilities for managing public access to geospatial data and information that could have significant homeland security implications.