

BIOGRAPHICAL INFORMATION

Brent A. Jones, PE, PLS

Vice President

James W. Sewall Company

Specific Responsibilities

Brent A. Jones provides senior level management oversight on all GIS energy and telecommunications projects and personnel at James W. Sewall Company. A professional engineer and land surveyor, Mr. Jones has expertise in civil and environmental engineering, utility design and construction management, and surveying/GPS, as well as extensive environmental permitting and regulatory compliance experience. Since 1996, he has supervised the development of electric, gas, and pipeline software applications for Sewall clients nationwide, overseeing GIS data conversion, database design, and proprietary software development. In addition to managing projects in utilities location, GIS landbase mapping, and addressing, Mr. Jones has brought to market modular software tools for pipeline alignment and schematic sheet generation, maximum allowable operating pressure (MAOP) calculation, class location analysis, high consequence area (HCA) and risk calculation, and leak detection.

Educational Information

B.S. – Surveying Engineering, University of Maine

Professional Memberships

GITA, Board of Directors

New England Chapter GITA, Past President

GIS for Oil & Gas Conference, Conference Chair (2002)

American Congress on Surveying and Mapping (ACSM)

Midwest Energy Association (MEA)

National Society of Professional Engineers (NSPE)

Identifying Sensitive Critical Infrastructure Data

Brent A. Jones, PE, PLS
Vice President
James W. Sewall Company
136 Center Street
Old Town, ME 04468
Telephone (207) 827-4456, Fax (207) 827-3641
Email: bjones@jws.com

ABSTRACT

Publicly available geospatial data usually lacks the detail and timeliness that terrorists require for planning an attack, according to a 2004 RAND report. Prepared by the RAND National Defense Research Institute for the National Geospatial-Intelligence Agency, this study found that geospatial data accessible on utilities, state government, and municipal Web sites is considered more sensitive than data available from federal sources.

How do utilities and governments at state and local levels determine if published data is sensitive? On what criteria do they base this determination? How do utilities share confidential critical infrastructure data in the event of an emergency? Does your utilities' data warrant restriction?

In this presentation, we will discuss a framework and methodology that can be used to assess whether publicly available geospatial information poses a risk to critical infrastructure, reviewing three key decision factors.

1. Risk to Security: Is your data useful to the adversary?
2. Uniqueness of Information: Is sensitive data unique to one data set?
3. Net Benefit of Disseminating Data: Does the benefit of distributing the data outweigh the risk?

We will also review current public and private data sharing mechanisms and explore the significance of the Freedom of Information Act (FOIA) and the Patriot Act on data access.

INTRODUCTION

The RAND National Defense Research Institute, a federally funded research and development center, prepared for the National Geospatial-Intelligence Agency a report titled "Mapping the Risks, Assessing the Homeland Security Implications of Publicly Available Geospatial Information." This report analyzes the issues associated with the terrorist use of publicly available geospatial information to attack critical infrastructure, providing a methodology for evaluating the sensitivity of this information.

According to the USA Patriot Act, critical infrastructure is defined as:

systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.¹

More specifically, the RAND report identifies critical infrastructure as food and water systems, agriculture, health systems and emergency services, information and telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons.²

How do we quantify the nation's critical infrastructure and how much of this infrastructure encompasses or relies on utilities, small and large, public and private? The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets cites the amount of critical infrastructure as follows:

- Agriculture and Food: 1,912,000 farms, 87,000 processing plants
- Water: 1,800 federal reservoirs, 1,600 municipal waste water facilities
- Public Health: 5,800 registered hospitals
- Emergency Services: 87,000 localities
- Defense Industrial Base: 250,000 firms in 215 industries
- Telecommunications: 2,000,000,000 miles of cable
- Energy:
 - 2800 electric power plants
 - Oil and Natural Gas: 300,000 producing sites
- Transportation:
 - Aviation: 5,000 public airports
 - Bridges: 590,000 highway bridges
 - Railroads: 120,000 miles of major railroads
 - Pipelines: 2,000,000 miles of pipelines
 - Maritime: 300 inland/coastal ports
 - Mass Transit: 500 major urban public transit operators
- Banking and Finance: 26,600 FDIC insured institutions
- Chemical Industry: 66,000 chemical plants
- Postal and Shipping: 137 million delivery sites
- Key Assets
 - National Monuments and Icons: 5,800 historic buildings
 - Nuclear Power Plants: 104 commercial nuclear power plants
 - Dams: 80,000 dams
 - Government Facilities: 3,000 government owned/operated facilities
 - Commercial Assets: 460 skyscrapers³

The interdependence of nonutility critical infrastructure with utilities is significant. Our banking and finance institutions, for example, rely heavily on our communications infrastructure for electronic transfer of funds, credit card and stock transactions, and the management and exchange of financial indices.

Because of the size and vulnerability of critical infrastructure, "key asset protection, is a shared responsibility that cannot be accomplished by the federal government alone. It requires coordinated action on the part of the federal, state, and local governments; the private sector, and concerned citizens across the country."³ Given that 85 percent of critical infrastructure is privately

owned, infrastructure owners and operators, including utility companies, are urged both to safeguard their facilities data and to share these data sets in emergency situations.

How do utilities and governments at state and local levels determine if published data is sensitive? On what criteria do they base this determination? How do utilities share confidential critical infrastructure data for emergency response and recovery? Does your utilities' data warrant restriction?

This paper addresses these questions, referencing the RAND methodology for determining sensitive geospatial data; reviews current public and private data sharing mechanisms; and explores the impact of federal acts on data access.

DATA ASSESSMENT METHODOLOGY

The RAND assessment methodology provides geospatial and data managers with a structured and consistent approach to identifying sensitive information, ensuring that all relevant factors are weighed, and a process and rationale for decision making. The methodology is based on the key criteria of *usefulness*, *uniqueness*, and *benefits and costs*.

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 nongeospatial 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?

DATA USEFULNESS

According to the RAND report, terrorists or potential attackers require geospatial information for both target selection and attack planning. Geospatial information used for target selection may include exact facility and materials storage locations such as a chemical plant and tank locations along with adjacent population information. Information for selecting a target may also include nongeospatial information that reveals the target's potential value. For example, \$300 million per day of goods cross the Ambassador Bridge, the international border crossing between Detroit, Michigan, and Windsor, Ontario. This information has the potential to aid a terrorist in determining the value of the target, but not in performing the attack. To plan the attack, such information as the target's exact location, layout, vulnerabilities, control centers, power sources, and security measures is useful. The RAND report clarifies the distinction between target-selection and attack planning information with the following questions:

Target-selection information	Which target? Where is it in general?
------------------------------	--

	What effect can the attacker achieve with a given class of attack and weapon?
Target and attack information	Is the target located where the attacker expects it to be such that the attack can be delivered effectively?
	What is the target made of, and how thick are the walls?
	What does the facility look like today, so the attacker can recognize it?
	Where are the guards, and how are they armed?
	Is there a quick reaction force?
	Is there a ditch that the attacker can use for cover?

Due to the level of accessibility of U.S. infrastructure and data, attackers have some flexibility as to where they can gather information to plan and carry out their attack. Focusing on federal data sources, RAND researchers determined that publicly accessible geospatial information is probably not the attackers' first choice. Publicly available information is useful for target selection and location, but lacked much of the information needed for most methods of attack. Certain attack methods require more detailed information (depending on target type, location, and other factors). The following table in the RAND report is included to help us consider what information a terrorist may need in each of the identified modes of attack.

Direct attack	Demolition charges Anti-material rifles Sabotage of sensitive components
Man-in-the-loop -precision attack	Suicide vehicular attack (air, land, sea) Suicide bomber Unmanned aerial vehicle (UAV) with data link for human operator
Autonomous precision attack	Aircraft using GPS/Inertial Navigation System (INS) UAV using GPS/INS Cruise missiles using GPS/INS Ballistic missiles using GPS/INS
Area attack	Chemical, radiological, biological agents from platforms Ad hoc chemical and radiological release Nuclear weapon

Although some of these attack modes are beyond the typical defense mechanisms of the average facility owner (e.g., missile attack, UAV), other attack modes can be deterred by restricting specific geospatial information. To deter a vehicular attack, for example, a facility owner may safeguard information on most of the ingress locations to a particular facility, but allow public access to information on the most protected and guarded entrance for visitors and deliveries.

There is a difference between the information an attacker needs to perform the attack (could not attack without it) and the information an attacker may use, but is not necessary to carry out the attack. In theory, lacking information required for a particular attack mode could deter the attacker from selecting a particular target. Terrorists are generally opportunistic, however, and can modify the mode of attack when faced with poor access to relevant and timely information.

The RAND report gives examples of information that is of high value for target selection and attack planning as follows:

Examples of Sensitive Information Types	Target Selection	Attack Planning
Internal Features		
- Control centers		X
- Power Sources		X
- Communication Lines		X
Engineering Details		
- Facility Construction	X	X
- Equipment layout and details		X
Operational Details		
- Day-to-day plant schedules	X	XX
- Security measures and practices	X	XX
Attack Assessment		
- Specific site consequences		X
- General impact (local or regional)	X	

(Note: A single “X” indicates that a particular type of sensitive information is likely to be considered desirable in meeting attackers’ information needs, while a double “X” indicates more highly desirable information.

Engineering details such as facility design drawings on dependent energy utilities and communication lines, for example, can reveal critical vulnerabilities that aids the attacker in selecting a specific target and planning the attack. The fact that such information on critical infrastructure is publicly available makes the target more attractive to the attacker because with more information the attacker has a higher probability of carrying out the attack.

DATA UNIQUENESS

Geospatial information is considered unique and a criterion for risk if the information is not available through other sources. Generally, geospatial data that indicates the location of vulnerable facilities in critical infrastructure is sensitive if not widely known. The general location of a pump station may be indicated on a municipal GIS Web site, but the critical nature of the station may not be. It is easily understood that the design drawings and piping diagrams are unique and are sensitive.

THE BENEFITS AND COSTS OF DATA SHARING

The last criterion to assess the sensitivity of geospatial data is the net societal benefits and costs of restricting public access. Before decisions to restrict access to geospatial data are made, it is important to weigh the expected benefits against the likely societal costs of restricting the data. These costs and benefits are difficult to gauge, but their analysis is crucial. Fire hydrants, for example, are part of the critical infrastructure, but restricting public access to their location will impact emergency responders and insurance companies as well. The benefits to public access to certain geospatial data outweigh the risk of distributing the information.

DATA SHARING

There is a changing relationship between infrastructure owners and the public sector. In emergency situations following a natural or manmade disaster, access to geospatial infrastructure

information for response planning and infrastructure recovery is essential. Traditionally the private sector has had concerns with sharing data with public agencies, namely because the data may become subject to the Freedom of Information Act (FOIA) and thus available to competitors. It can be argued that private critical infrastructure data is not subject to FOIA because an exemption protects private companies against disclosures of trade secrets and confidential business information. Further, provisions in the Critical Infrastructure Information Act of 2002 (CIIA) establish limitations on the disclosure of critical infrastructure information voluntarily submitted to the Department of Homeland Security (DHS).⁴ The CIIA was enacted to respond to the need for the federal government and facility owners and operators to share information related to vulnerabilities and threats, and to promote data sharing.

These provisions do not necessarily apply to other types of geospatial data that are potentially critical in an emergency, but not considered part of the critical infrastructure data. Address information, land base mapping and associated orthophotography may not contain sensitive critical infrastructure data, but they are decidedly competitive assets to a private company. If this noncritical data is shared with the government, it is possible to become subject to FOIA—a concern to infrastructure owners. To obviate the problem, many infrastructure owners are using data license agreements that allow sharing and updating of land base mapping information that prevent the data from entering the public domain. Common land base and addressing systems are essential and greatly aid the use of geospatial data, especially when responding to an emergency and time is critical. Often geospatial data developed at differing accuracies has limited use. Certain recovery efforts are not feasible without compatible geospatial data; efforts can be frustrating and time consuming to plan and coordinated recovery efforts can be stymied.

As homeland security and interagency/public-private critical infrastructure emergency response and recovery planning matures, formal data sharing agreements that permit the sharing of sensitive data will become standard in communities that develop emergency response plans and will include all of the critical infrastructure owners.

SUMMARY

There is a renewed awareness of the size, nature, and vulnerability of the nation's critical infrastructure. Understanding modes of attack and identifying information used in target selection and attack planning assist in determining what information may be considered sensitive. With geospatial technological developments, geospatial, facility, and descriptive data can be made easily accessible to an ever-widening audience. Using the methodology developed by RAND, critical infrastructure owners and operators can assess the sensitivity of the data that they share or make public by applying the criteria of *usefulness*, *uniqueness*, and *the cost/benefit of restricting access*. The federal government has made provisions regarding sharing sensitive critical infrastructure data with the DHS, but sharing sensitive data on the local level is still subject to ad hoc agreements. The new emergency response goals dictate close sharing of geospatial data among shareholders that have not necessarily coordinated in such ways in the past. When agencies and neighboring companies begin to plan geospatial and critical infrastructure data coordination, how will you participate?

NOTES

1. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, HR 3162 RDS, 107th Congress, 1st Session, U.S. Senate, 24 October 2001.
2. *Mapping the Risks, Assessing the Homeland Security Implications of Publicly Available Geospatial Information*, RAND National Defense Research Institute, RAND Corporation, 2004.
3. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, The White House, Washington D.C., February 2003.
4. *Homeland Security Act of 2002: Critical Infrastructure Information Act*, Report for Congress, 28 February 2003.