

RISK & INSURANCE®

Emerging Strategies for Risk

AP PHOTO: MANUEL BALCE CENETA



FEDERAL CONTRACTORS face the risk of a congressional investigation when something goes wrong. Here, Deputy Veterans Affairs Undersecretary, retired Army Brig. Gen. Michael J. Kussman (center), and Robert Seliger (far left), CEO and co-founder of Sentillion Inc., along with other U.S. Dept. of Veterans Affairs managers testify in June before at a House of Representatives hearing on safeguarding medical information.

● INSURANCE

Working a Federal Case

Information-technology firms should work with agents, brokers and insurers to help understand the unique exposures of doing contract work for the federal government. BY JIM WEST

Information technology is integral to the U.S. government's delivery of services to people and businesses throughout the world. In today's post-Sept. 11, 2001, environment, expenditures on security and national defense—two areas that rely heavily on information technology—comprise an even larger percentage of the federal budget.

Also, the federal government is increasingly reliant on private-sector contractors that have specialized knowledge to meet its needs. It is no surprise, then, that the federal government is the world's largest purchaser of IT products and services, ranging from over-the-counter software to highly specialized and often classified

programs for government agencies.

This dependence on private contractors for IT products and services is likely to deepen. For example, federal spending on IT outsourcing initiatives is projected to increase 8 percent each year through 2010, according to the latest forecast by Input, a Virginia market-research company. The research firm expects this segment of the industry to reach \$17.6 billion in revenue in 2010, up from \$12.2 billion today.

Federal government IT contractors face a variety of unique risks and challenges, ranging from work performed on military equipment to installing hardware to support battlefield communications to supplying data-mining software used to identify potential terrorist suspects. Through the Department of Health and Human Services, Veterans Affairs and other programs, the federal government also maintains the largest number of medical records in the world.

FEDERAL GOVERNMENT IT CONTRACTORS FACE A VARIETY OF UNIQUE RISKS AND CHALLENGES, RANGING FROM WORK PERFORMED ON MILITARY EQUIPMENT TO INSTALLING HARDWARE TO SUPPORT BATTLEFIELD COMMUNICATIONS TO SUPPLYING DATA-MINING SOFTWARE USED TO IDENTIFY POTENTIAL TERRORIST SUSPECTS.

Given this diversity of operations, many federal government IT contractors specialize in one particular technology or governmental agency. Being disciplined and knowing the ins and outs of each agency help both the agency and the federal government IT contractor comply with Federal Acquisition Regulation, or FAR. This governmentwide regulation requires that all expenditures with appropriated funds be properly documented and accounted for. Failure to comply with FAR may result in a variety of penalties, from political reprimands to congressional inquiries for the agency to fines and, ultimately, disqualification of the federal government IT contractor.

THE LURE OF IMMUNITY

If the world of federal government IT contractors seems unduly difficult, there is one possible compensating feature: the potential for government immunity. The U.S. Supreme Court has recognized the "military contractor defense," also known as the "government contractor defense," most recently in 1978. This defense protects contractors from tort liability for products or services manufactured or delivered in accordance with the U.S. government design specifications. The U.S. government only offers immunities when national security is at stake.

In 2002, Congress passed the SAFETY Act, as part of the Homeland Security Act, which was designed to create an incentive for manufacturers to develop anti-terrorism technology by shielding them from potential liability. The act creates certain liability limitations for claims arising from, relating to or resulting from terrorism where qualified technologies have been deployed to prevent, detect or lessen the impact of a terrorist attack.

Insurance brokers who represent federal government IT contractors often cite the potential for immunity to explain why their clients face a low level of risk. Without a thorough understanding of how these protections work, such assumptions can be dangerously wrong. Federal government IT contractors and their brokers should work with a knowledgeable underwriter to craft a portfolio of insurance policies that reflect the exposures and advantages such contractors have when working for the federal government.

RISK ASSESSMENT

Insurers writing this business find it requires much more than the typical desk underwriting transaction. Assessing risk

here can be much more difficult than for a standard commercial line.

Consider the following scenarios:

- A federal government IT contractor is installing and testing satellite communications software on a \$15 million piece of government-owned property. Under FAR guidelines, the contractor is responsible for all loss of or damage to the property.

- A federal government IT contractor working for the Department of Defense is awarded a cost-plus contract to install marine buoys after the release of environmental contaminants. Contractors are occasionally awarded contracts for work that exceeds their operational capacities.

- A federal government IT subcontractor is sued by the prime contractor for nonperformance. Federal government IT contractors normally have contractual obligations with entities other than the federal government.

- A federal government IT contractor is providing remote storage of patient records for the Department of Health and Human Services. The contractor may be held liable if these records are lost or stolen.

- A federal government IT contractor is supplying technical programming services in support of a classified Department of Defense contract. If the contractor is unable to disclose the scope, duration or cost of the contract, the insurance policy may be cancelled.

The products and services that federal government IT contractors provide tend to be extremely complex and diverse. For example, many of these contractors do a great deal of research and development for the Department of Defense and for federal intelligence agencies, laboring on electrical systems, software, communications systems and hardware, creating prototypes or even taking those prototypes all the way through to production. Against this backdrop, all parties involved must exert greater diligence in understanding the nature of these varied products and services so that accurate judgments of risk can be assessed.

In addition, underwriters often can't obtain full disclosure of exactly what the IT products and services are intended to

do for the Department of Defense, the National Security Agency or the Central Intelligence Agency, among others, because the information is classified. In coping with this, agents, brokers and underwriters need specialized knowledge coupled with the ability to ask the right questions in such a way that risk assessment information can still be gathered without compromising the project's classified status. While this task is difficult, it can be accomplished by insurance professionals with years of experience in this line.

Another issue to consider is the distinct possibility that an IT product or service developed for the federal government could end up on the commercial market. In fact, many do. When a federal government IT contractor does develop a commercial application for his product, any immunity that may have been granted under the government agreement will no longer apply, and product-liability exposures will become real. Therefore, contractors need to think through this possibility from the very start and be mindful of this exposure down the line.

Diversity of company operations is an additional consideration. Quite a few private-sector firms work exclusively on government contracts. A number of others operate mainly in the government sector, but also sell a portion of their products on the commercial market. In the latter case, immunity for the government work is not likely to protect all of the operation. Federal government IT contractors require experienced insurers that have the technical know-how to sort through these diverse exposures, many of which may potentially involve different lines of insurance. Consistently satisfying the insurance needs of these contractors requires underwriting experience, expertise and time. While the level of due diligence is greater in this area than in other commercial areas, so are the rewards.

JIM WEST is senior vice president, Chubb & Son, and manager of Chubb's Information and Network Technology segment. He can be reached at riskletters@lrp.com.