## THE PENTAGON

# RETHINKING THE SAFETY OF SOFTWARE CODED OVER THERE

**UNTIL NOW,** the debate over the exodus of software programming to places like India has mostly focused on whether lower costs are worth lost American jobs. Now, however, a new hot-button issue is surfacing—about whether such outsourced programming is a threat to national security.

A Pentagon task force is in the final stages of preparing recommendations on how to deal with the fact that some software the military buys from American companies is coded offshore. The task force is part of the **Defense Science Board,** an advisory group made up of volunteers from the military and industry. While the task force's deliberations are secret, the conversations its members have been having with outside experts are raising concerns in the tech industry about what the recommendations will be.
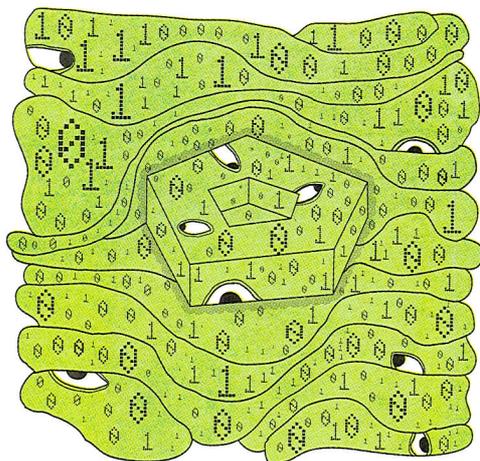


"We recognize that there are real threats," says Phillip Bond, chief executive of the **Information Technology Association of America,** a lobbying group. "We want government to deal with this in a smart way, and we're concerned they might do it wrong."

The worry is that the Pentagon might enact policies forcing tech suppliers to break off pieces of their global supply chains, making it difficult for American companies to deliver the most advanced products to the Pentagon at affordable prices. These days, computer builders, chipmakers, software publishers, and tech-service outfits all tap inexpensive programming talent in foreign countries.

A government effort to fence out offshore suppliers, they fear, could bring a return to the days when too much of the stuff the Pentagon bought was custom-made—a practice made infamous by the government's much-publicized procurement of $600 toilet seats and other absurdly priced items in the early 1980s.

It's not clear yet if the tech industry's fears will be realized. William Schneider Jr., chairman of the Defense Science Board (but not a task force member), says he's confident that the recommendations won't be draconian—or over-reaching. "We're concerned with the use of high-end, mission-critical software and the process with which it gets written," Schneider told *BusinessWeek.*

There are no easy solutions, since pieces of software created offshore are embedded throughout computing equipment and software packages sold by U.S. companies. Besides, making sure the Pentagon's highly networked tech gear is secure goes beyond the issue of offshore programming. After all, Americans can be hackers and spies, too. Says Paul Kaminsky, another Defense Science Board member: "With networks, often it's the inside threat that gets you."

*–Steve Hamm and Dawn Kopecki*

## QUESTION OF THE WEEK

What would a Democratically controlled Congress mean for business, the economy, or your industry?
*– Cliff Edwards and Dawn Kopecki*

*"Monetary policy and the long-run fiscal outlook-they'd be unchanged. The big economic effect would be in sectors with a great relationship with the White House now–oil, defense contractors, pharma."*
Justin Wolfers, asst. professor, business and public policy, the Wharton School

*"Whoever wins, the new Congress has to tackle policies on intellectual property, health care, and immigration, an issue that's tearing us apart because it's unresolved. And vocational education, which is abysmal in this country."*
Andy Grove, cofounder, Intel

*"Are changes in Washington coming? Probably. But it's important for both parties to remember that Americans who suffer from illness don't sign in at the hospital as Republicans or Democrats."*
Billy Tauzin, president and CEO, Pharmaceutical Research & Manufacturers of America; former Congressman (R.-La.)