

## GOVNET Won't Solve U.S. Government Internet Security Concerns

**Instead of developing a new, separate U.S. government network to replace part of the Internet, federal officials should focus on improving performance, security and survivability.**

---

**Event:** On 11 October 2001, Richard Clarke, the newly appointed adviser to U.S. President George W. Bush for "Cyberspace Security," promoted the concept of a separate government Internet to enable more secure communications among agencies and federal workers. The new GOVNET network would be distinct from the public Internet to keep it safe from viruses, hackers and terrorists. Clarke's office issued a request for information for vendors to respond to the initiative.

**First Take:** At first glance, a government-only Internet appears to make sense. It has meritorious goals — high performance, a high level of security and survivability. However, the federal government already uses several networks for military and nonmilitary communications. Therefore, the General Services Administration, charged with procuring services for the federal government, should carefully examine whether GOVNET would be redundant to existing networks and, thus, become a costly waste of time and resources.

Presidential Decision Directive 63 promises that the U.S. government would become a model security citizen on the Internet. Moving to a physically separate GOVNET would require the government to unhook from the Internet without ever trying to live up to the directive's goals. Gartner believes that rather than retreat from secure use of the public Internet, the government should focus on the required security technologies, processes and purchasing discipline to ensure that the government conducts all its uses of the Internet securely and reliably, and uses its buying power to have security services built into offerings for the provision of Internet service. Where the Internet fails to meet its needs, the government should look to *enhance* rather than *replace* its private networks. Lastly, the government should consider piloting an ARPANET-like initiative on next-generation security and survivability technologies that might identify enhanced security benefits for both government and commercial networks. (ARPANET, the Advanced Research Projects Agency Network, was the forerunner of the Internet.)

If GOVNET gets funded, defense contractors, network providers and security vendors should view it as a short-term opportunity to sell products and services to a private network. Enterprises and government agencies should assume that a long-term solution to Internet security will arise elsewhere and should proceed to buy denial-of-service protection and other managed security services from commercial providers.

**Analytical Source:** John Pescatore, Information Security Strategies, and Jay Pultz, Enterprise Network Strategies

Written by Michael Gomez, gartner.com

### Gartner

The content herein is often based on late-breaking events whose sources are believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of the information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The conclusions, projections and recommendations represent Gartner's initial analysis. As a result, our positions are subject to refinements or major changes as Gartner analysts gather more information and perform further analysis. Entire contents © 2001 Gartner, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden.