



Setting the Standard for Automation™

InTech provides the most thought-provoking and authoritative coverage of automation technologies, applications, and strategies to enhance automation professionals' on-the-job success.

InTech.

 [Login](#)

[InTech Home](#) → [InTech Home](#)

23 September 2008

InTech Home

Feature Articles

[Article Index](#)

Columns & Departments

[Association News](#)
[Automation Basics](#)
[Automation Update](#)
[Certification Review](#)
[Channel Talk](#)
[Executive Corner](#)
[Government News](#)
[Products and Resources](#)
[Standards](#)
[Talk to Me](#)
[The Final Say](#)
[Workforce](#)
[Development](#)
[Your Letters](#)
[Archives of Prior Departments](#)

InTech e-News

[Business News](#)
[e-News Archives](#)
[Events](#)
[Industry News](#)
[Pinto's Points](#)
[Blog](#)

General Information

[About InTech](#)
[Advertise in InTech](#)
[Mailing Lists](#)
[Subscribe](#)
[Contact Us](#)
[ISA Home](#)



GAO report: U.S. needs to pep up cyber security efforts

The organization responsible for protecting the country from cyber attacks needs to develop a warning system that truly works, according to a Government Accountability Office (GAO) report.

The problem is the United States Computer Emergency Readiness Team (US-CERT) does not have a comprehensive cyber analysis and warning capability, according to the report. The GAO identified 15 keys a system would need spread across monitoring, analysis, warning, and response.

While US-CERT's cyber analysis and warning capabilities include aspects of each of the key attributes, they do not fully incorporate all of them. As a part of its monitoring, US-CERT does garner information from numerous external information sources. But it has not established a comprehensive baseline of our nation's critical computer-reliant critical assets and network operations. In addition, while it investigates if identified anomalies constitute actual cyber threats or attacks as part of its analysis, the organization does not integrate its work into predictive analyses, nor does it have the analytical or technical resources to analyze multiple, simultaneous cyber incidents. The organization also provides warnings by developing and distributing a wide array of attack and other notifications; however, these notifications are not consistently actionable or timely—providing the right information to the right persons or groups as early as possible to give them time to take appropriate action. Further, while it responds to a limited number of affected entities in their efforts to contain and mitigate an attack, recover from damages, and remediate vulnerabilities, the organization does not possess the resources to handle multiple events across the nation.

The report notes there has been a proliferation of threats to computer networks and the sensitive information stored and transmitted from them as the Internet has increasingly become critical to everyone. These threats range from hackers breaking into a network for bragging rights to serious threats from foreign intelligence services and terrorists, which seek to disrupt and destroy U.S. critical infrastructure.

"U.S. authorities are concerned about the prospect of combined physical and cyber attacks, which could have devastating consequences," according to the GAO. "For example, a cyber attack could disable a security system in order to facilitate a physical attack."

The GAO had 10 recommendations for the Department of Homeland Security (DHS), which houses US-CERT, in establishing a comprehensive national cyber analysis and warning capability. DHS agreed with nine out of the 10 recommendations but disagreed with the GAO's final recommendation to ensure "there are distinct and transparent lines of authority and responsibility assigned to DHS organization with cyber security roles and responsibilities."

DHS responded it had already satisfied the recommendation in an earlier concepts-of-operation document. The GAO said the document is still in draft and has no date for finalization or implementation.

For related information, go to www.isa.org/productivity.

All contents copyright of ISA © 1995-2008 All rights reserved.

[Find Local Sections](#) | [ISA Home](#) | [Report a Problem](#) | [Privacy & Legal Policies](#) | [Site Map](#) | [Help](#) | [Contact Us](#)

ISA | 67 Alexander Drive, Research Triangle Park, NC 27709 USA | (919) 549-8411