

New U.S. Government Security Guidelines Need More Clarity

John Pescatore, Jay Heiser

New Office of Management and Budget incident-reporting guidelines represent a step forward for U.S. government information security. But the government's definitions of security incidents are still too imprecise to be truly effective.

Event

On 12 July 2006, the U.S. Office of Management and Budget (OMB) issued a memorandum to CIOs of federal government agencies that tightens the reporting-timeliness requirements for some security breaches and other incidents involving personally identifiable information. The memorandum also restated OMB requirements — in effect since 2000 — that all funding for information technology systems include security. The memorandum is available online at www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf.

Analysis

Gartner believes that the new OMB memorandum is primarily a public-relations response to recent high-profile security incidents. Nevertheless, we think it represents a positive change in U.S. government information security policy. Federal agencies are now required "to report all incidents involving personally identifiable information to US-CERT [the United States Computer Emergency Readiness Team] within one hour of discovering the incident." The National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (SP 800-61) previously mandated one-hour US-CERT reporting for all Category 1 (unauthorized access) incidents, but allowed weekly reporting for less-serious Category 4 (improper usage) incidents. An improper-usage incident — such as the detection of sensitive personal information on a home computer or other unsupported device — must now be reported within one hour. This will reduce the possibility that such incidents will be reported in the news media before being formally reported by the relevant government agency. Gartner believes, however, that "improper usage" is not defined clearly enough as it relates to personal information, and that either the OMB or NIST should issue more specific guidance in this area.

The OMB memorandum also specifies that federal government CIOs "should report all incidents involving personally identifiable information in electronic or physical form and should not distinguish between suspected and confirmed breaches." This is a positive step, because it removes the temptation to wait for confirmation that information has actually been used or compromised. However, increased and faster reporting will lead to little more than accurate and timely statistics unless incident response processes in government are drastically improved.

Recommendations for government agencies

- Review your incident-reporting processes to determine whether the new one-hour requirement can be met, and develop streamlined reporting processes if it cannot.
- In the absence of specific OMB/NIST guidance on what constitutes improper usage, review your existing definitions to ensure that they are explicit and clearly understood by security staff and other personnel.
- Ensure that all information technology procurements contain funding for application of information security processes.

Analytical Sources: John Pescatore and Jay Heiser, Gartner

RECOMMENDED READING

- "Essential Incident Response Activities During the First 24 Hours" — Enterprises must be prepared to act quickly to limit the damage of attacks during the critical first day. **By Amrit Williams, Greg Young and Jay Heiser**
- "Findings From 'Security and Risk' Meeting: Augment FISMA Reporting With Technical Controls to Improve Operational Security" — Federal Information Security Management Act compliance can be an opportunity to improve an enterprise's security posture. **By Amrit Williams and John Pescatore**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509