April 2007

PRIVACY

Lessons Learned about Data Breach Notification

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-657, a report to congressional requesters

Why GAO Did This Study

A May 2006 data breach at the Department of Veterans Affairs (VA) and other similar incidents since then have heightened awareness of the importance of protecting computer equipment containing personally identifiable information and responding effectively to a breach that poses privacy risks. GAO's objective was to identify lessons learned from the VA data breach and other similar federal data breaches regarding effectively notifying government officials and affected individuals about data breaches. To address this objective, GAO analyzed documentation and interviewed officials at VA and five other agencies regarding their responses to data breaches and their progress in implementing standardized data breach notification procedures. The cases at the other agencies were chosen because, like the VA case, they involved loss or theft of computing equipment and relatively large numbers of affected individuals (10,000 or more).

What GAO Recommends

To better ensure that individuals who are at risk of identity theft are offered consistent levels of support, GAO is recommending that the Director of OMB develop guidance for agencies on when to offer credit monitoring and when to contract for an alternative form of monitoring, such as data breach monitoring, to assist individuals at risk of identity theft. In written comments on a draft of this report, OMB and VA concurred with GAO's recommendation.

www.gao.gov/cgi-bin/getrpt?GAO-07-657.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda D. Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Based on the experience of VA and other federal agencies in responding to data breaches, GAO identified the following lessons learned regarding how and when to notify government officials, affected individuals, and the public:

- Rapid internal notification of key government officials is critical.
- Because incidents vary, a core group of senior officials should be designated to make decisions regarding an agency's response.
- Mechanisms must be in place to obtain contact information for affected individuals.
- Determining when to offer credit monitoring to affected individuals requires risk-based management decisions.
- Interaction with the public requires careful coordination and can be resource-intensive.
- Internal training and awareness are critical to timely breach response, including notification.
- Contractor responsibilities for data breaches should be clearly defined.

These lessons have largely been addressed in guidance issued in 2006 from the Office of Management and Budget (OMB), which is responsible for overseeing security and privacy within the federal government. However, guidance to assist agency officials in making consistent risk-based determinations about when to offer credit monitoring or other protection services has not been developed. Without such guidance, agencies are likely to continue to make inconsistent decisions about what protections to offer affected individuals, potentially leaving some people more vulnerable than others.