



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, 8 PVL 1606, 11/09/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Corporate Security

Updated Accounting Privacy Principles Add Risk Management, Portable Devices Criteria

OTTAWA—The finalized update to the U.S.-Canada business accounting practices privacy principles framework incorporates a key new risk management criterion to help businesses recognize and address risks to the personal information they hold, a Canadian Institute of Chartered Accountants (CICA) spokesman told BNA Nov. 5.

The latest version of the Generally Accepted Privacy Principles (GAPP) document, developed by the CICA and the American Institute of Certified Public Accountants, includes a new criterion that requires businesses to use a risk assessment process to establish a risk baseline and to conduct at least annual reassessments to identify new or changed risks to personal information, Nicholas Cheung, the CICA's principle for assurance services development, told BNA.

“Organizations really need to understand where they are so they understand their threats and weakness and what they need to address,” he said.

A second key addition to the GAPP framework is a new security criterion that requires organizations to protect from unauthorized access any personal information that is stored on portable media or devices, he said. This responds to the many technological advances since the last GAPP update in 2006 (6 PVL 108, 1/22/07), and particularly the proliferation of portable devices such as laptop computers, he said.

Ongoing updates to the GAPP framework are critical, as the public concern over the growing number of privacy breaches highlights the significant concerns over the protection of personal information, Cheung said. The framework responds to those concerns by addressing internal processes for data protection, he added. “Most of the breaches are caused by internal factors, not external factors,” according to Cheung. “Hopefully

the framework will help reduce the number of causes for internal breaches.”

The document was finalized in August but not formally released until Nov. 5.

New Requirements, Modifications. The updated GAPP document adds a total of eight new criteria and removes one criterion, bringing the total to 74. It modifies three others. In addition, it modifies one of the 10 original principles on which GAPP is based by adding proper data disposal to the existing principle addressing the use and retention of personal information.

The other changes to GAPP criteria include new requirements to:

- identify potential types of personal information and sensitive personal information and the processes for handling them, and to include that information in privacy and security policies;
- document privacy incident and breach management programs;
- provide a privacy awareness program;
- inform individuals of the acquisition of additional information on them;
- dispose of information that is no longer retained to be anonymized, disposed of, or destroyed in a safe manner;
- establish ongoing procedures to monitor the effectiveness of controls on personal information and to take timely corrective actions.

The latest GAPP document expands the criterion for infrastructure and systems management to restrict the use of personal information in process and systems testing. It modifies the information security program criterion to require organizations' security programs to include references to ISO/IEC 27002:2005, which provides a code of practice for information security management. It eliminates the criterion on escalation of complaints and disputes on the basis that it duplicates the criterion for dispute resolution and recourse.

The accounting privacy framework was originally developed in 2003 by a joint privacy task force established by the two national institutes (2 PVL 406, 4/21/03), and

was rebranded in May 2006 as GAPP. The latest update is based on an extensive consultation process, including the release for public comment of several draft versions (8 PVLR 504, 3/30/09; 8 PVLR 747, 5/18/09).

Privacy: Good for Business. The GAPP document notes that it is based on the underlying premise to the 10 privacy principles it identifies that good privacy is good business and a key component of proper corporate governance and accountability. Maintaining the privacy of personal information collected and held by an organization is a top business imperative, particularly since increasingly complex and sophisticated business and systems and processes collect ever-growing amounts of personal information, it said.

“Because more data is being collected and held, most often in electronic format, personal information may be at risk to a variety of vulnerabilities, including loss, misuse, unauthorized access, and unauthorized disclosure,” it said.

Managing privacy risk for organizations operating in a multi-jurisdictional environment can be even more difficult, and although the GAPP document provides an operational framework to help organizations’ management to address privacy in a way that takes into consideration many local, national, or international requirements, adherence to it does not guarantee compliance with all laws and regulations to which organizations may be subject, it said.

“Although this framework provides guidance on privacy in general, organizations should consult their own legal counsel to obtain advice and guidance on particular laws and regulations governing an organization’s specific situation,” it said. “Organizations need to be aware of the significant privacy requirements in all of the jurisdictions in which they do business.”

BY PETER MENYASZ

The finalized GAPP document is available at <http://op.bna.com/pl.nsf/r?Open=byul-7xhufa>.