The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) has announced publication of the free, Web-based _CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS_ edited by Elizabeth B. Lennon. The following is a slightly-edited quotation from the release note circulated to subscribers of the _ITL Bulletin for June 2002_ (used with permission of the editor).

NIST's Information Technology Laboratory has published a recommended guidance document on contingency planning for federal departments and agencies. Industry will find the recommendations valuable as well. NIST Special Publication (SP) 800-34, which provides guidance to individuals responsible for preparing and maintaining IT contingency plans. The guide discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of IT systems, and provides examples to assist readers in developing their own IT contingency plans. The document, among others, is available in a printable Acrobat PDF file at <http://csrc.nist.gov/publications/nistpubs/index.html>. While you are there, note the extensive links on the left column of that page, including "Alerts", which brings you to a useful list of current vulnerability alerts called the "Vulnerability and Threat Portal."

The IT contingency planning guide identifies fundamental planning principles and practices to help personnel develop and maintain effective IT contingency plans. The principles meet most organizational needs; however, each organization may have additional requirements specific to its own processes. The document provides guidance to help personnel evaluate information systems and operations to determine contingency requirements and priorities. The guidance also provides a structured approach to aid planners in developing cost-effective solutions that accurately reflect their IT requirements and integrate contingency planning principles into all aspects of IT operations.

The guidance presented should be considered during every stage of contingency planning, starting with the conceptualization of contingency planning efforts through plan maintenance and disposal of the contingency plan. If used as a planning management tool throughout the contingency planning process, the document and its appendices should provide users with time- and cost-saving practices.

The guide presents contingency planning principles for the following common IT processing systems:

* Desktop computers and portable systems (laptop and handheld computers)

* Servers * Websites

* Local area networks (LANs)

* Wide area networks (WANs)
* Distributed systems

* Mainframe systems.

The document discusses common technologies that may be used to support contingency capabilities. Given the broad range of IT designs and configurations, however, as well as the rapid development and obsolescence of products and capabilities, the scope of the discussion is not intended to be comprehensive. Rather, the document describes practices for applying technology to enhance an organization's IT contingency planning capabilities.

The document outlines planning principles that may be applied to a wide variety of incidents that could affect IT system operations. The scope includes minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period. Because IT systems vary in design and application, specific incident types and associated contingency measures are not provided in the document. Instead, the planning guide defines a process that may be followed for any IT system to identify planning requirements and develop an effective contingency plan.

* * *

Readers may subscribe to the ITL Newsletter in ASCII e-mail format by sending an e-mail message from your business e-mail account to <mailto:listproc@nist.gov> with the message "subscribe itl-bulletin" (not including the quotation marks). To have the Bulletin delivered to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or send a request to <mailto:elizabeth.lennon@nist.gov>.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.