Everyone benefits from knowing how other people manage their security policies. At a recent conference, I was introduced to the Federal Best Security Practices (BSPs) that are currently being collected by the CIO Council of the United States government. The Web site <http://bsp.cio.gov/> provides a list of the 20 policies that have been contributed so far, some descriptive information about the project, and forms for submitting proposals for new BSPs.

In the definitions and framework page <http://bsp.cio.gov/BSPDefined.cfm>, the CIO Council defines a BSP as, "an existing method, proven effective and validated by actual experience, that people use to perform a security-related task." Their contrast between what a BSP is and is not is instructive for anyone thinking about security policies:

A BSP

* Is a "human practice; that is, a repeated or customary method used by people to perform some action."
* Is not "an IT security mechanism, which is implemented by hardware, software, or firmware although such tools are often essential components of a BSP."

* Is "security-related; that is, plays a part in protecting an organization's information, resources, or at a business operations."
* Is not "a business practice, though it supports the organization's business operations."

* Is "Proven-effective in achieving a security objective as the result of actual operational experience."
* Is not "a best possible practice but a best existing practice; not the result of armchair theorizing.

* Among the most effective of existing practices used to perform a particular security process."
* Is not "necessarily the single best existing practice of a particular sort."

The definitions and security frameworks page includes useful links to a number of Federal Government security frameworks:


* Security of Federal Automated Information Resources (Appendix III to OMB Circular No. A-130) <http://www.whitehouse.gov/OMB/circulars/a130/a130.html> from the Office of Management and Budget;


System Security Engineering Capability Maturity Model <http://www.sse-cmm.org/> from the National Security Agency;

The list of the current Federal BSPs <http://bsp.cio.gov/list.cfm> provides visitors with 20 documents. A few of these interesting and valuable papers are as follows:

Securing POP mail on Windows clients <http://bsp.cio.gov/getfile.cfm?messageid=00020> comes from NASA and discusses practical methods for securing common e-mail software;

Integrating security into the systems development lifecycle <http://bsp.cio.gov/getfile.cfm?messageid=00013> is from the Social Security Administration;

How to deploy firewalls <http://bsp.cio.gov/getfile.cfm?messageid=00009> from the Software Engineering Institute at Carnegie Mellon University;

Continuity of operations <http://bsp.cio.gov/getfile.cfm?messageid=00008> from the Department of the Treasury.

I encourage all readers to make use of all of the BSPs in planning or updating their own security policies and procedures. I hope that all agencies of the US Federal Government will submit their own contributions to the CIO Council for inclusion in this expanding library.

* * *

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.

Copyright © 2001 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.