BEST SECURITY PRACTICES: AN OVERVIEW

Guy King

Computer Sciences Corporation, Defense Group,
Information Security and Operations Center

5113 Leesburg Pike, Suite 902 gking1@csc.com
Falls Church, VA 22041 703/575-5115

"By nature, [humans] are nearly alike;
by practice, they get to be wide apart."
--Confucius, *Analects*.

Abstract: Security technology is important to security, but the practices of the people who develop, integrate, evaluate, configure, maintain, and use that technology are more important; indeed, these practices are the foundation of technical (as well as physical and personnel) security. It is crucially important, therefore, that security practices be good ones; when feasible, *best security practices* (BSPs) should be used. In Section 2 this paper defines "BSP," asserts the need for multiple levels of goodness among BSPs, and connects the sharing of BSPs to Knowledge Management. Section 3 argues for the use of a *security process framework* (SPF) to categorize BSPs and describes an SPF that harmonizes three well-known collections of BSPs. Section 4 identifies six important phases, or functions, of the BSP life cycle–namely, identify, package, evaluate, adopt, deliver, and improve–and briefly discusses packaging (offering a format for BSPs) and evaluation (discussing some criteria for such evaluation). A summary concludes the paper.

Keywords: best practice, best security practices, administrative security, security process framework, knowledge management.

1: Introduction[1]

"Things are in the saddle, /And ride [hu]mankind," Emerson wrote in 1846 [6]; how much truer his words today! The computer-based information revolution has taken off, and information technology (IT) is riding us hard. This holds true of our own field: when information systems security is mentioned, people think first of security technology–firewalls, intrusion detection software, virus scanners. It is too little appreciated that, as important as such technology is, even more important are ***the practices of the people*** who develop, integrate, evaluate, configure, maintain, and use that technology. Indeed, good security practices are the *foundation* of security, for technical (as well as physical and personnel)

1 This paper is based on work performed under the Principal Resource for Information Management Enterprise-wide (PRIME) Contract for the U.S. Agency for International Development (USAID). This work included participating in the PDD 63 Best Practices and Standards Working Group (see [13]) and supporting the Security Practices Subcommittee (SPS) of the Federal CIO Council. [15], which was developed by USAID for the SPS with funding from the Government IT Services IT Improvement Fund, contains a more complete account of the matters discussed here. The CIO Council's Best Security Practices Web site, at http://bsp.cio.gov, also reflects this material and contains actual best security practices. The views presented here are solely those of the author and not necessarily those of USAID.

safeguards are secure only if the practices of the people who develop, administer, operate, and maintain them are secure.

Since the early 1990s, practitioners in various subject areas have begun to recognize the importance of *best practices*: practices that have proven effective when used by one or more organizations and which, therefore, promise to be effective if adapted by other organizations. In the past two years there has been an increasing recognition of the need for *best security practices* (BSPs) to protect U.S. critical infrastructures, information, and business operations. By identifying BSPs, then sharing them with other organizations, one cost-effectively leverages security knowledge.

The remainder of this paper is organized so:

Section 2: defines "BSP," asserts the need for multiple levels of goodness among BSPs, and connects the sharing of BSPs to Knowledge Management.
Section 3: argues for the use of a *security process framework* (SPF) to categorize BSPs and describes an SPF that harmonizes three well-known collections of BSPs.
Section 4: identifies six important phases, or functions, of the BSP life cycle–namely, identify, package, evaluate, adopt, deliver, and improve–and briefly discusses packaging (offering a format for BSPs) and evaluation (discussing some criteria for such evaluation).
Section 5: concludes with a summary.

2: What Is A Best Security Practice?

Security requirements can be implemented by several means:

- *Technical*: software, hardware, or firmware (i.e., information technology [IT]);
- *Physical*: physical barriers, locks, etc.; and
- *Administrative*: the actions and practices of people.

BSPs fall under the heading of administrative safeguards.

Table 1 defines "Best Security Practice." Column 1 says what a BSP is, and column 2 lists a few of the things it is not.

Table 1. "Best Security Practice" Defined

A BSP Is…	
A human practice; that is, a repeated or customary method used by people to perform some process	**Not** an IT security mechanism, which is implemented by hardware, software, or firmware
Security-related; that is, plays a part in protecting an organization's information, resources, or business operations	**Not** a business practice, though it supports the organization's business operations
Shown by experience to be effective in performing some security process; the result of operational experience	**Not** a best *possible* practice but a best *existing* practice; **not** the result of armchair theorizing
***Among* the most** effective of those existing practices used to perform a particular security process	**Not** necessarily *the single* best existing practice of a particular sort

In summary, a **best security practice (BSP)** is a human practice shown by experience to be among the most effective of those existing practices used to perform a particular security process.

A documented BSP will describe the steps people are to take in performing the security process and will optimally include template and sample documents, checklists, and other such aids. To better help those who would adapt it, a documented BSP may also include other material, including a statement of its purpose, success stories, relationship to other BSPs, implementation guidance and resource estimates, metrics, tools, and training materials. (See Section 4.1 below, "Packaging BSPs.")

The first three attributes of "BSP" (named in Table 1) follow from analysis of the term itself. The fourth ("*among* the most effective") is included for reasons now to be explained.

2.1: From Best to Worst

"The best is the enemy of the good," wrote Voltaire [16]. If we pursued the goal of identifying and mandating *the single* best way to perform each security process, we would show our agreement with Voltaire. It takes but a little experience and reflection, though, to teach that practices are context-sensitive, hence, they do not apply equally (work equally well, have the same effects) in all circumstances. For example, for some organizations, in some circumstances, the best may not be cost-effective; in these cases, to put it paradoxically, the good may be better than the best. To put it more plainly, sometimes the good is good enough. This argues for the collection of both best and good security practices.

For example, Chevron Oil Company recognizes four levels, as follows:

"1. GOOD IDEA -- Unproven: not yet substantiated by data but makes sense intuitively; could have a positive impact on business performance. Requires further review/analysis.
2. GOOD PRACTICE -- …has been implemented and has improved business results for an organization….This is substantiated by data collected at the location.
3. LOCAL BEST PRACTICE -- …has been determined to be the best approach for all or large parts of an organization …, based on an analysis of process performance data. The analysis included some review of similar practices outside of Chevron….
4. INDUSTRY BEST PRACTICE -- …has been determined to be the best approach for all or large parts of an organization…based on internal and external benchmarking, including the analysis of performance data" [2:28-29].

Note that Chevron's levels are of varying degrees of excellence; and that they are identified using evaluation criteria of differing levels of stringency (for example, analysis of local performance data, internal and external benchmarking). The less stringent criteria (as in #1 above) provide less *assurance* that the practice truly is good, while the more stringent criteria (as in #4) provide more assurance.[2]

2 Although Chevron varies the stringency of the evaluation criteria *directly* with the degree of goodness (the greater the goodness, the more stringent the evaluation criteria), others may choose to make these two independent of one another.

Security stakeholders would even profit from knowing what the *worst* security practices are, for "The best plan is to profit by the folly of others" [11:Bk. xviii, sect. 3].

2.2: BSPs and Knowledge Management (KM)

When we speak of sharing BSPs, we are talking about sharing knowledge; and here knowledge includes know-how.

As KM experts have learned, sharing know-how is difficult, for the reason that much know-how is tacit: a person with know-how may be unable to articulate his or her know-how. Some things cannot be said; they can only be shown. KM experience confirms that to share best practices, it is not enough to document the practices (as fully as possible) and place them on a Web site; it is necessary, further, to provide face-to-face interaction between experts and novices, as with the masters and apprentices of medieval guilds.[3]

3: Security Process Framework (SPF)

Government and Industry sources agree that the use of a process framework facilitates the sharing as well as the management of best practices.[4] A process framework also "provide[s] a common vocabulary for people from different" organizations to identify similar processes [2:19].

An SPF is closely related to the more familiar notion of a **security program**. A security program is a comprehensive set of program areas (e.g., risk management, personnel security, security training) that, together, guide an organization's actions to protect its information resources.

Each **program area** (or high-level security process) is a cluster of related security sub-processes. For example, the contingency planning program area includes, among others, the sub-process (a) Develop a contingency plan; and it, in turn, includes the sub-processes (a_1) Identify and prioritize business functions, (a_2) Analyze resources needed by those business functions, (a_3) Identify the time frames in which each resource is needed, (a_4) Identify a likely range of problems each resource may experience, (a_5) Plan emergency response to those problems, and so on. (See [9:3.6].)

Together the program areas and their sub-processes provide a **security process framework**--an ordered structure of security processes, used to categorize BSPs. By identifying the security processes that need to be performed, the SPF maps the security terrain and thus helps answer the question "Has my organization addressed 10%, or 50%, or 80%, of the needed processes?" The SPF also facilitates the management of BSPs and–if used on a Web site to organize BSPs–can guide customers in their search for BSPs to match their needs.

BSPs are needed within each program area, for each security sub-process. For example, a BSP describing how to identify and prioritize business functions would be useful to someone developing a contingency plan (see paragraph before last).

Frameworks specifically for security processes exist, implicitly, in several major efforts to identify best security practices:[5]

3 See, e.g., [5] and [2].
4 See, e.g., [7:"Introduction"], [3], [1:19-20], and [8:"Executive Overview"].

5 These efforts do not identify their process frameworks as such; but they do organize BSPs by means of security processes (or what can alternatively be described as security processes).

- SSE CMM *Model Description Document* [14]
- NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* [9]
- British Standard 7799, *A Code of Practice for Information Security Management* [4]

The SPFs implicit in these three documents differ from one another. Because none offers rationalia justifying their choices of processes, none provides grounds for our preferring it to the other two. Analysis indicates, however, that the high-level processes shown in Figure 1 harmonize the high-level processes of all three.

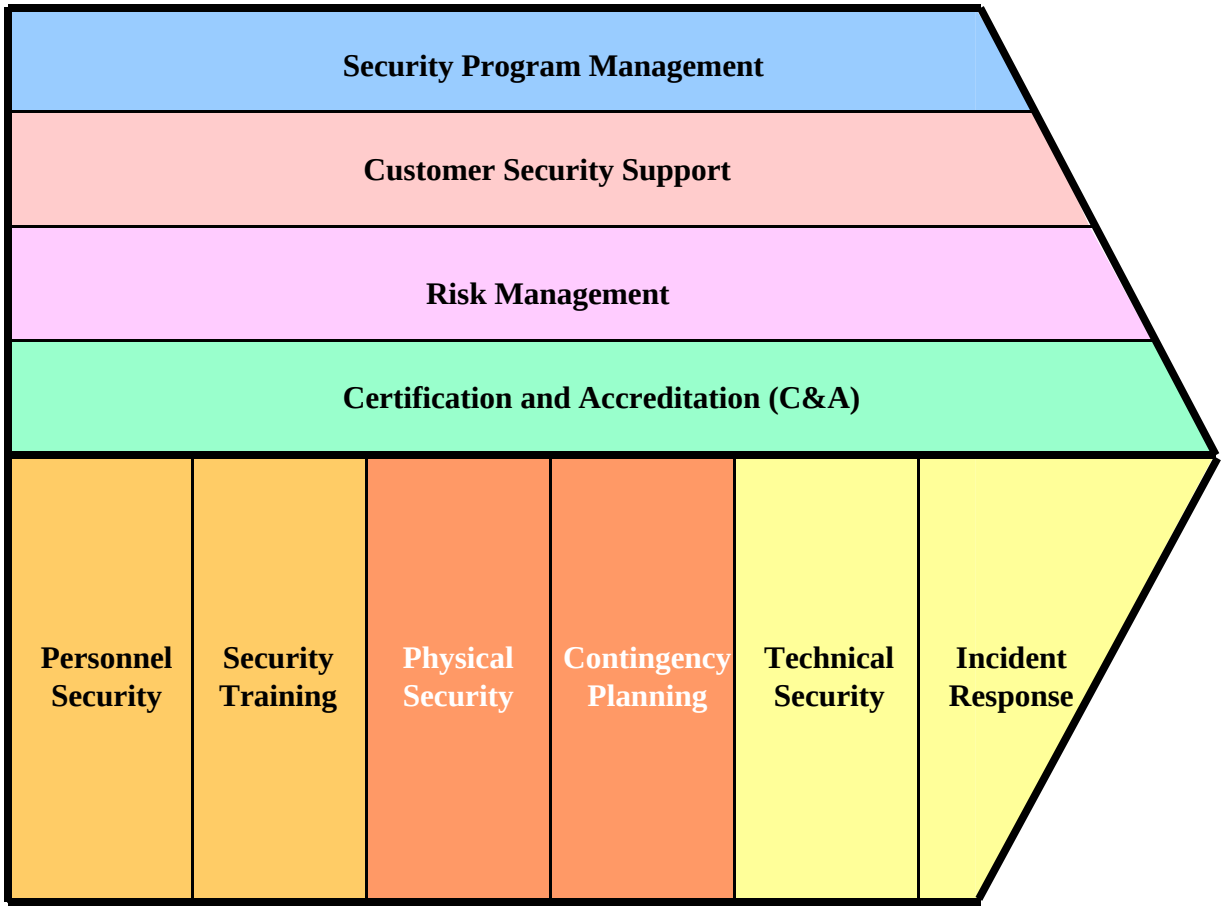

Figure 1. The Ten High-Level Processes of the SPF

Figure 1 follows the conventions established by Michael Porter [12], wherein the processes named in the bottom half provide 'line' security functionality and the processes named above are *support* functions.

The structure of the SPF is grounded in the interrelations of its ten processes. As its name suggests, security program management is an umbrella process that controls the other nine processes. Three of the remaining nine processes are closely involved in security program management:

- Customer security support is integral to security program management as well as to the other eight processes.

- Risk management and C&A apply to personnel, physical, and technical security; that is, when one performs risk management and C&A, one examines personnel, physical, and technical security safeguards.

Personnel, physical, and technical security jointly contribute to the security both of organizational security programs and of information systems. Security training, contingency planning, and incident response are actually major sub-processes of those three, respectively.

Two observations lead to a complication in the SPF:

- The development and operation of an *organizational* security program is distinct from the development and operation of secure *information systems*. For example, an organizational security program provides, as it were, a security infrastructure that is used by the organization's information systems security programs. The BSPs useful in developing and operating an organization security program will differ from those BSPs useful in developing and operating a secure information system. However, the same high-level processes (e.g., personnel security, physical security, risk management, security training) are relevant both to organizational and to information systems security programs.
- All of the highest level security processes have a life cycle. As the preceding paragraph indicates, however, the life cycle of the high-level security processes of an organizational security program is distinct from the life cycle of the high-level security processes of an information system. See Figure 2 on the relations between the two life cycles.

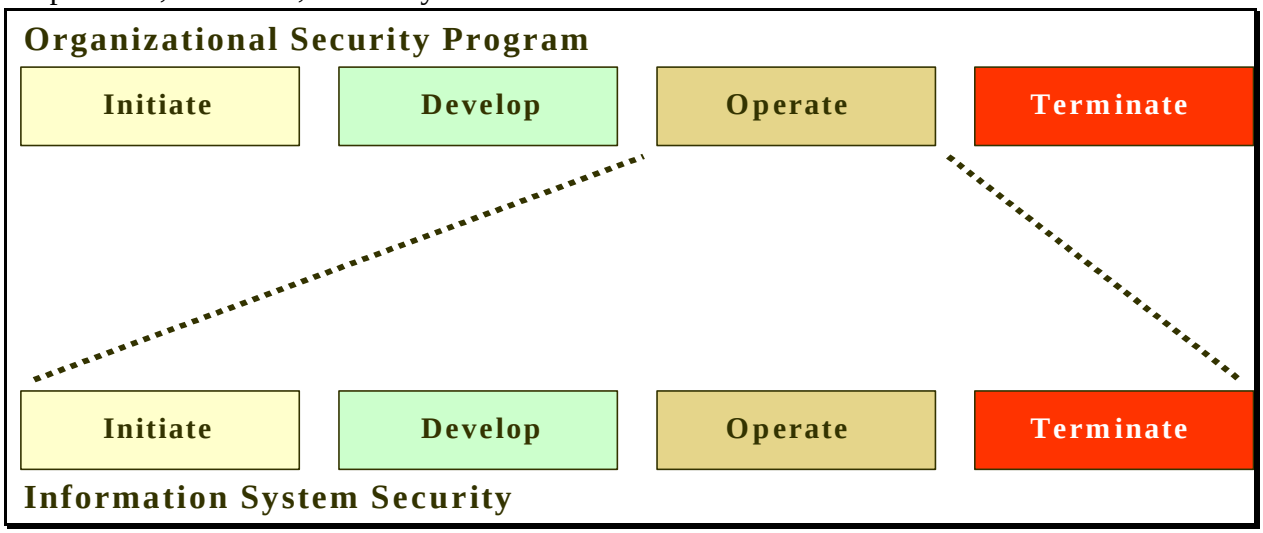

Figure 2. The life cycles of an organizational security program and of information systems are distinct: the Operate phase of the former life cycle guides all phases of the latter.

Because of these two observations, the SPF has the structure shown in Table 2. The life-cycle phases are those of OMB A-130.

Table 2 The SPF has two major divisions, *Organizational Security Program* and *Information System Security*; and the ten security processes of each division follow a four-phase life cycle.

SPF, Part 1: ORGANIZATIONAL SECURITY PROGRAM				
Security Process Areas	*Life Cycle Phases*			
	Initiate	Develop	Operate	Terminate
Security Program Mgmt				
Personnel Security				
Security Training				
Physical Security				
Contingency Planning				
Technical Security				
Incident Response				
Risk Management				
C&A				
Customer Security Support				
SPF, Part 2: INFORMATION SYSTEM SECURITY				
Security Process Areas	*Life Cycle Phases*			
	Initiate	Develop	Operate	Terminate
Security Program Mgmt				
Personnel Security				
Security Training				
Physical Security				
Contingency Planning				
Technical Security				
Incident Response				
Risk Management				
C&A				
Customer Security Support				

This is more complicated than one would like, of course. It would be nice to cut the SPF off at just the ten high-level processes. But the ugly facts expressed in the two observations above prevent our doing that. Likewise, when one tries to map all of the BSPs from the three BSP collections mentioned above to the ten processes, one is again driven to this complexity.

It is easy to see how Table 2's appearing on a Web site could help guide users to the BSPs they seek. Users would click within the cells intersecting the process areas and life-cycle phases to find the associated BSPs.

4: BSP Life Cycle

BSPs have a life cycle. If we ignore the two important functions (or phases) of BSP *creation* and BSP *adaptation* (the latter by using organizations) and look at the BSP life cycle from the point of view of an organization seeking to collect and make them available for use by others, six

life-cycle functions stand out, as shown in Figure 3.

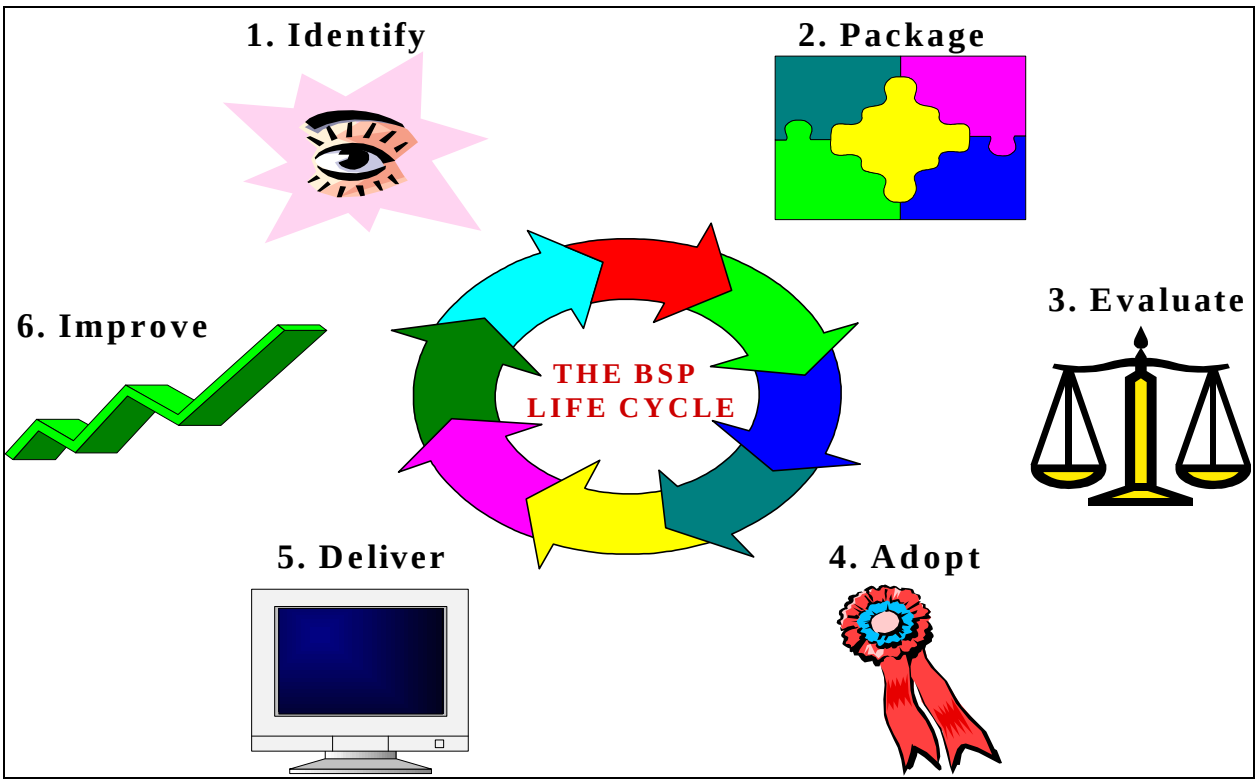

Figure 3. Six Functions of the BSP Life Cycle

Table 3 defines these six functions and states why each is needed.

Table 3. Definition of and Rationale for the BSP Life Cycle Functions

The Function Defined	*Why the Function Is Needed*
***Identify Candidate BSPs**: through research and solicitation, collect security practices that have some claim to being effective*	BSPs are produced by others and so must be obtained from them.
***Package BSPs:** document BSPs according to a standard format*	A standard format ensures that BSPs include the information sought by users and needed to help them apply the BSPs to their circumstances.
***Evaluate BSPs:** assess BSPs against some set(s) of criteria, in order to determine whether and to what degree they really are good*	Because ignorant or malicious persons may claim that mediocre or even harmful SPs are good, and because some good SPs are significantly better than other good SPs, BSPs must be evaluated for actual, relative goodness.

The Function Defined	Why the Function Is Needed
Adopt BSPs: *with advice of evaluators, approve the use of BSPs by the community of users*	If the evaluation of BSPs is performed by a third party, the BSP managers may wish to retain some control of the results. Adoption is separated from evaluation to support this concept.
Deliver BSPs: *make BSPs available to users via the Web, CDs, hardcopy, help desk, and traveling experts*	To ensure that each user, regardless of circumstance, is able to access and use the BSPs, multiple delivery mechanisms should be used. Because technical means alone do not suffice, people-to-people interactions are needed.
Improve BSPs: *maintain BSPs to keep them current with relevant drivers and to incorporate improvements suggested by the user community*	Laws, technology, business needs, and vulnerabilities change, and BSPs must change to keep pace. Also, like all human products, BSPs will be imperfect and in need of improvement. A BSP may go through multiple releases, each an improvement over the last.

Space constraints restrict us here to the consideration of just two of these functions: packaging and evaluation.

4.1: Packaging BSPs

Table 4 presents a comprehensive format for BSPs.

Table 4. A Standard Format for BSPs

Section of BSP Package	Content / Use of this Section
1.0 Identification Data	
1.1 BSP Number	A unique number associated with this BSP
1.2 BSP Name	Name of this BSP
1.3 Version Number	Number (e.g., 1.1) of this release of this BSP
1.4 Date Adopted	Date this BSP was adopted
1.5 Approving Authority	Name and role of the approving authority
1.6 Source of BSP	Organization which originated this BSP
1.7 Level of BSP	Level of goodness and/or assurance of this BSP
1.8 Security (Sub-)Process / Framework(s) Supported	Security (sub-)process(es) supported by this BSP, and the framework(s) (e.g., SPF) within which the (sub-)process is found
1.9 Reserved	
1.10 Point of Contact (POC)	Name, telephone number, facsimile number, email address, and city/street address of person to contact for more information regarding this BSP
2.0 What This BSP Does	
2.1 Purpose of BSP	Briefly states the purpose of the BSP, to help users decide whether this BSP is the one they seek, the one that will help them do what they need done
2.2 Requirements for this BSP	Quotes the security requirement(s) which the BSP helps satisfy and cites their source

Section of BSP Package	Content / Use of this Section
2.3 Success Stories	Describes the results achieved by those who have used the BSP, and how to contact them
3.0 What This BSP Is	
3.1 Description of Best Practice	This is the heart of the BSP; it describes the inputs, constituent activities, and outputs of the BSP
3.2 Relationship to Other Best Practices	Identifies other BSPs related to this BSP and characterizes their relations
4.0 How To Use This BSP	
4.1 Implementation Guidance	Provides lessons learned by those who have implemented this BSP; designed to help users better implement this BSP
4.2 Implementation Resource Estimates	Summarizes the resources required to implement the BSP, according to those who have implemented it
4.3 Performance Goals and Indicators (Metrics)	States performance goals this BSP has achieved, and the metrics used to measure them
4.4 Tools	Identifies and briefly describes tools associated with the use of this BSP; may provide a URL(s) where the tools may be found
4.5 Training Materials	Identifies and briefly describes materials to train those who will use this BSP; may provide a URL(s) where the materials may be found
Appendices	
A Executive Overview and Briefing	Contains materials which can be used to brief managers on the use of this BSP
B Reference List	A list of books, articles, and URLs where one can learn more about the BSP
C Procurement Information	Information about available contract vehicles by which one can procure items related to this BSP
D Evaluation Information	Summarizes how this BSP was judged qualified to be a BSP of this level
E Recommended Changes	Lists the changes that users have recommended for the next version of the BSP

It is reasonable to ask the BSP contributor to complete the unshaded (yellow) sections. If the BSP contributor does not complete all of these sections, the BSP managers may complete them; the BSP managers will also complete the shaded (gray) sections. BSP contributors must complete all mandatory sections; the section headings underlined in column 1 indicate sections that should probably be mandatory.

4.2: Evaluating BSPs

The BSP evaluation function examines BSPs to determine whether they have indeed been effective in performing some security sub-process, and likely, therefore, to be effective elsewhere in the future. To use terminology made familiar by the Government Performance and Results Act (GPRA), BSPs are evaluated for relative *performance*. The *metrics* upon which the

evaluation is based are experiential ("performance-based").

A review of other efforts to evaluate best practices suggests that the following are useful criteria for evaluating BSPs. Compared to other practices used to perform the same security sub-process, a BSP:

- Improves the ability of the organization to achieve its security and business goals
- Reduces costs
- Saves time
- Is easy to implement

Obviously, some BSPs may score high with respect to one criterion and low with respect to another.

BSP evaluation is potentially a costly operation. Happily, when a BSP is evaluated, only a few of the subsections of the BSP format need be scrupulously evaluated–namely, those subsections making claims of effectiveness, namely:

1.7 Level of BSP [Goodness]
2.4 Success Stories
4.3 Performance Goals and Indicators (Metrics)

Besides checking for effectiveness, the evaluation ought to check the BSP for consistency with other BSPs. Section 3.2 of the standard BSP format identifies related BSPs; the consistency check can focus on these BSPs.

The evaluation ought also to assess whether the documented BSP reveals any vulnerabilities in the contributing or using organizations.

In addition, all BSPs, regardless of level of goodness (including 'candidate' BSPs, which some BSP managers will release to users before they have been evaluated for effectiveness), ought to be evaluated against the following minimum criteria: the BSP contributors are who they claim to be (their contact information is correct), the mandatory sections of the BSP are complete, and the BSP has been reviewed for *prima facie* plausibility/reasonability and seems unlikely to cause harm.

5: Conclusion

The shortage of skilled security practitioners in both Government and Industry is critical. Education is one important response to this problem. Sharing BSPs is another.

In sharing and managing BSPs, it is advisable to use a security process framework such as that shown in Table 2; to employ a standard BSP format such as that in Table 4; and to plan to support the six BSP life-cycle functions named in Figure 3.

References

[1] APQC, "Benchmarking: Leveraging 'Best Practice' Strategies: A White Paper for Senior Management"; available at http://www.apqc.org/best/bmk.

[2] APQC, "Identifying and Transferring Internal Best Practices" by Carla O'Dell and C. Jackson Grayson; available at http://www.apqc.org/download.htm.

[3] APQC, *Process Classification Framework*, developed by APQC's International Benchmarking Clearinghouse in partnership with Arthur Andersen & Co., SC; available at http://www.apqc.org/free.

[4] BS 7799-1, *Information Security Management–A Code of Practice for Information Security Management*, British Standards Institution, 1999.

[5] Denning, Stephen, "What Is Knowledge Management"; available at http://www.apqc.org/download.htm.

[6] Emerson, Ralph Waldo, "Ode Inscribed to W.H. Channing," 1846; reprinted in *Selections from Ralph Waldo Emerson*, Stephen E. Whicher, ed., The Riverside Press: Cambridge, Mass., 1957.

[7] *Government Process Classification Scheme: A Taxonomy of Common Government Processes to Use for Collecting and Sharing "Best Practices,"* v1.01, October 1, 1996; available at http://www.va.gov/fedsbest/KB.htm.

[8] Information Systems Audit and Control Foundation, *CobiT Framework*, April 1998, 2nd edition; available at http://www.isaca.org/down.htm.

[9] NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, Marianne Swanson & Barbara Guttman, September 1996; available at http://cs-www.ncsl.nist.gov/nistpubs.

[10] OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, "Security of Federal Automated Information Resources," February 1996; available at http://www.whitehouse.gov/WH/EOP/OMB/html/circulars/a130/a130.html.

[11] Pliny the Elder, *Natural History*, Loeb Classical Library, Harvard University Press, 1991.

[12] Porter, Michael, *Competitive Advantage: Creating and Sustaining Superior Performance*, The Free Press, 1985.

[13] Steinauer, Dennis, *et al.*, "Best Security Practices for US Government Information Systems" Panel, NISSC, Washington, D.C., October 20, 1999.

[14] *Systems Security Engineering Capability Maturity Model (SSE CMM) Model Description Document*, v2.0, April 1999; available at http://www.sse-cmm.org.

[15] USAID, *Proposed Plan for the Federal Best Security Practices (BSPs) Program (FBSPP)*, February 19, 2000.

[16] Voltaire, *Dictionnaire Philosophique*, "Dramatic Art," 1764.