Generally Accepted System Security Principles

Release for Public Comment

Ralph Spencer Poore

The Generally Accepted System Security Principles (GASSP) Committee has approved this release of the GASSP for public comment. The introductory materials and the sections through and including Section 2.1 *Pervasive Principles* are included for the reader's information only. *Pervasive Principles* have previously had a public comment period. The GASSPC asks the profession to review and comment on Section 2.2 *Broad Functional Principles* (the majority of the document). Section 2.3 *Detailed Security Principles* remains a work in progress that will be built on the *Broad Functional Principles*. We welcome your comments on all aspects of the document; however, we ask that you concentrate on substantive matters rather than editorial.

The Chairman asks that we provide special recognition to all those persons and organizations that have contributed to the GASSP effort to date. In addition, he cites the following individuals and organizations for their exceptional contributions: Craig Schiller, who drafted the first strawman in a Herculean original effort; the Computer Security Institute (CSI), which has consistently provided the GASSPC with solid support; the Massachusetts Institute of Technology (MIT), which has provided the GASSPC with a Web site; Charlie LeGrande and the Institute for Internal Auditors (IIA) for the same reason; as well as William H. Murray, Ian Ross, Hal Tipton, Ross Leo, and Ralph Poore. These organizations and individuals made major contributions, often at significant personal sacrifice.

Please address your comments to Ralph Spencer Poore at rspoore@ralph-s-poore.com with a copy to Will Ozier, Chairman, GASSPC at wozier@pacbell.net. The public comment period will end 90 days after publication. ■

Generally Accepted System Security Principles

The International Information Security Foundation (I^2SF)-Sponsored Committee to Develop and Promulgate Generally Accepted System Security Principles

BACKGROUND

Formation of the I^2SF-sponsored GASSP Committee (GASSPC) began in mid-1992 in response to Recommendation #1 of the report *Computers at Risk (CAR)*, published by the United States of America's National Research Council in 1990. That recommendation, "To Promulgate Comprehensive Generally Accepted System Security Principles," and its subordinate elements sparked the genesis of a concerted effort to establish a well-balanced committee population representing key elements of the private and public sectors from both the United States and abroad.

Both administrative and product-related principles are being addressed, individual and organizational privacy rights are being addressed, and, to consolidate all the elements of a rapidly evolving industry, alliances are being established to the International Information Systems Security Certification Consortium $(ISC)^2$, the international Common Criteria effort to develop information technology product-related information security principles, and other organizations having an interest in the security of information and associated principles.

To consolidate and sustain the value of comprehensive GASSP effectively, the CAR recommendation envisions the creation of an authoritative infrastructure to maintain the GASSP, support their evolution, enforce "compliance," and provide a vehicle for the authoritative approval of reasonably founded exceptions or departures from GASSP. This authoritative infrastructure would be modeled after those that support and sustain the Generally Accepted Accounting Principles (GAAP) and like models of the international accounting profession.

The GASSP Committee kickoff meeting was held in the United States at the 1992 National Computer Security Conference in Baltimore, Maryland, and was attended by 25 leading information security experts from the United States, Canada, the United Kingdom, France, Germany, the Netherlands, Sweden, and the European Commission (EC). Many differing perspectives and agendas were discussed in an open exchange, but at the close of the meeting, it was the consensus that the objectives were important, necessary, and, perhaps most significant, achievable.

BENEFITS

☐ The GASSP will promote good practice.
☐ The GASSP will provide the authoritative point of reference and legal reference for information security principles, practices, and opinions.
☐ Good information security practice will increase the effectiveness and efficiency of business, promote trade and commerce, and improve productivity.
☐ Good information security practice will help preserve the necessary public trust in the ability to leverage modern information technology while avoiding unintended consequences. This trust is necessary for the effective use of the technology.
☐ The GASSP will improve the effectiveness and the efficiency of the information technology security functions and practitioners by promoting the best practice and reducing duplication of creative effort.
☐ Global harmonization of information security principles will serve to minimize artificial barriers to the appropriately free flow of information that can result from conflicting standards and controls.
☐ Information security professionals are practitioners certified and self-policed against a Common Body of Knowledge (CBK) maintained through coordination between the GASSP infrastructure and $(ISC)^2$. Thus, a globally known skill set will be assured.
☐ Management will have increased confidence that information security practitioners' decisions are in concert with GASSP.
☐ Industry and government will be motivated to support GASSP, recognizing the broad efficiency achievable through the recognition of globally accepted GASSP.
☐ Management worldwide will hold functional information security to the same set of rules.
☐ Vendors will be able to develop products with global conformance, rather than meeting variable local guidance, thus reducing both development and end-use costs.
☐ Vendor products conforming to GASSP will enjoy increased customer confidence, trust, and acceptance.

APPROACH

Rather than another *ad hoc* effort, the GASSPC decided to establish an Authoritative Foundation of existing works that, through their broad acceptance, have articulated, in one way or another, the GASSP of the information security profession. Recognizing the hierarchic nature of principles, it was determined to use the Organization for Economic Cooperation and Development (OECD) Information Security Principles, with their international acceptance, as the model for the foundation of the GASSP hierarchy, the Pervasive Principles, and, through a careful analysis and mapping of the Authoritative Foundation and derivative works, to develop Broad Functional Principles, as accepted and supported by consensus of the IT industry and profession. Finally the GASSPC will develop Detailed Principles, including "how to" guidance.

The development of a consensus-building process is central to the success of this approach. Other key tasks include the establishment of linkages to the Common Criteria and the $(ISC)^2$-sponsored CISSP designation.

Finally, two essential elements, which will be evolutionary in nature, are to be developed. The first is the definition and establishment of an authoritative infrastructure, or governing body. This effort has been initiated. Second is the development of models for legislative/regulatory initiatives that have the support of the profession, industry, and government. Their purpose will be to establish the "glue" that effectively binds the consolidation of these complex issues internationally.

OBJECTIVES

☐ The international harmonization of culturally neutral information security.
☐ The elimination of artificial barriers to the free flow of information worldwide.
☐ The definition and implementation of a principled foundation for an industry, the success of which is critical to the future of the Information Age and its ramifications for privacy and security.

☐ Provision for the rapidly evolving nature of information security methods, issues, and technology, and their articulation in principle.
☐ Recognition and correlation to related management issues.

CURRENT STATUS

[*Note*: This section articulates current project status. In the final document, this section will be replaced with a development history.]

The National Performance Review (NPR) Task Force, formed by the Vice President of the United States of America, has recommended that the National Institute of Standards and Technology (NIST), with advice from the National Security Agency (NSA) and the Office of Management and Budget (OMB), develop GASSP for the federal government. The GASSPC has drafted strategic project plans to secure funds that will enable the GASSPC to accelerate its efforts and develop GASSP that NIST, in turn, can adapt in response to its NPR task. It is essential now to secure funding and "in kind" support, identify a fund administrator, and support the working GASSP project team as appropriate.

The GASSP Pervasive Principles, based on the OECD principles, have been developed, based on comments received and addressed to the GASSPC-approved Exposure Drafts, 1.0 and 2.0, which were published for comment and widely circulated. Work has begun on defining and mapping the GASSP Broad Functional Principles. A fully articulated outreach and awareness program is also under way.

Core tasks of the GASSP Project and their status are as follows:

☐ Define and execute the outreach and awareness program (ongoing).
☐ Research and complete the GASSPC Foundation Documents List (ongoing).
☐ Develop and approve the framework for the GASSP (completed).
☐ Map the GASSPC Foundation Documents List of related authoritative works (ongoing).
☐ Survey the industry to ascertain outside interest/support (ongoing).
☐ Define/establish liaison with the International Information Systems Security Certification Consortium $(ISC)^2$ (completed).
☐ Define and approve the Consensus Process I (Internal-GASSPC) and II (External) (completed).
☐ Develop Exposure Draft 1.0 of the GASSP Pervasive Principles, approve, and release for public comment (completed).
☐ Address public comment to GASSP Pervasive Principles ED 1.0, approve, and release as GASSP Pervasive Principles Version 1.0 for public comment (completed).
☐ Address public comment to GASSP Version 2.0, submit to the GASSPC for final review and comment, and release, without GASSPC voting member objection, as GASSP Version 2.0 (in process).
☐ Extract and define GASSP Broad Functional Principles from the GASSPC foundation Document List and map to Pervasive Principles (completed).
☐ Execute the Consensus Process on GASSP Broad Functional Principles (completed).
☐ Plan development of GASSP Detailed Principles (pending).
☐ Execute development of GASSP Detailed Principles (pending).
☐ Define/establish liaison with the Common Criteria Project (pending).
☐ Define, approve, and establish the GASSPC governing infrastructure, the International Information Security Foundation (I^2SF) (initiated).
☐ Fund and populate the I^2SF (pending).

THE GASSP INTERNATIONAL COMMITTEE MEMBERS

Belgium

☐ David Herson — *European Commission,* information only

Canada

☐ Peter Davis — *Peter Davis & Associates,* voting member
☐ Peter Kingston — *The Kingston Group,* voting member and liaison for Canadian Information Processing Society (CIPS)

☐ Ian Ross — *Communications Security Establishment*, voting member

France

☐ Yvon Klein — *Centre National d'Etudes Spatial*, voting member

Germany

☐ Ulrich van Essen — *Bundesamt für Sicherheit in der Informationstechnik*, voting member

Japan

☐ Haruki Tabuchi — *Fujitsu Limited*, voting member
☐ Junji Tezuka — *JEIDA*, observer

Mexico

☐ Miguel Alvarado — *CONSI Group*, voting member
☐ Ana Dominguez — *Cabletron*, voting member

Netherlands

☐ Fritz Taal — *National Communications Security Agency*, voting member

Sweden

☐ Mats Ohlin — *Defense materiel Administration*, voting member

United Kingdom

☐ Nigel Hickson — *Department of Trade and Industry*, voting member

United States

☐ Jim Appleyard — *IBM Corporation*, voting member and liaison for SHARE
☐ Tom Austin — *IBG Corporation*, voting member
☐ Laura Brown — *Ernst & Young LLP*, voting member
☐ Stephen A. Carlton — *Security Analysts Incorporated*, voting member and liaison for the Standing Committee for the Safeguarding of Proprietary Information of ASIS
☐ Cris R. Castro — *Ernst & Young LLP*, voting member
☐ Lawrence Champion — voting member and liaison for the Computer Security Committee of ASIS
☐ Ken Cutler — *Information Security Institute*, observer
☐ Jim Flyzik — *Department of the Treasury*, information only
☐ Brian Kahin — *Office of Science and Technology Policy*, information only
☐ John Kinyon — *Motorola Incorporated*, observer
☐ Charles Le Grand — *The Institute of Internal Auditors*, voting member and liaison for IIA
☐ Ross Leo — *Dynegy, Inc.*, voting member
☐ Landa McLain — *PricewaterhouseCoopers LLP*, observer
☐ William Hugh Murray — *Deloitte & Touche LLP*, voting member
☐ Peter G. Neumann — *SRI International*, information only
☐ Christopher Nichols — *Ernst & Young LLP*, voting member
☐ Kristen Noakes-Fry — *Noakes-Fry Associates*, voting member
☐ Thomas J. Orlowski — *National Association of Manufacturers*, voting member and liaison for NAM
☐ Will Ozier — *OPA, Inc.–The Integrated Risk Management Group*, chair and voting member
☐ Donn Parker — *SRI International*, voting member
☐ Chuck Perkins — *PricewaterhouseCoopers LLP*, voting member
☐ Ralph S. Poore — *Ernst & Young LLP*, voting member
☐ Jeffrey Reich — *Dell Computer Corporation*, voting member
☐ Craig Schiller — *SAIC*, voting member
☐ Hal Tipton — *HFT & Associates*, voting member
☐ Fred Tompkins — *National Computer Security Association*, voting member
☐ Dan White — *Ernst & Young LLP* (formerly), voting member
☐ Lauren Wood — *AlliedSignal*, voting member and liaison for the International Standards Organization (ISO)

Generally Accepted System Security Principles (GASSP) Version 2.0 June 1999

The International Information Security Foundation (I^2SF)-Sponsored Committee to Develop and Promulgate Generally Accepted System Security Principles

ACKNOWLEDGMENTS

Special thanks is due to the GASSP Committee, to organizations that established liaisons with the GASSP Committee, and to the various organizations that employ the GASSP Committee members for their contributions, comments, and support in this voluntary endeavor. The effort of the GASSP Committee and the support of their respective employers were essential in the preparation of this document.

1.0 INTRODUCTION

Information security is a combination of preventive, detective, and recovery measures. A preventive measure is a risk control that avoids or deters the occurrence of an undesirable event. Passwords, keycards, badges, contingency plans, policies, firewalls, and encryption are examples of preventive measures. A detective measure is a risk control that identifies the occurrence of an undesirable event. Visitor logs, audit trails, motion sensors, closed-circuit TV, and security reviews are examples of detective controls. Detective measures also provide a means for reporting the occurrence of events. A recovery measure is a risk control that restores the integrity, availability, and confidentiality of information assets to their expected state. Examples of recovery measures are fault tolerance, backup, and disaster recovery plans.

Information security also includes education, awareness, and training measures that inform computer users of the "acceptable use" principles and practices that support the protection of information assets. The introduction of GASSP supports and strengthens these controls. These principles should be constructed to ensure that the information system reduces the possibility of a risk event and its impact.

1.1 PURPOSE

The GASSP Committee seeks to develop and maintain GASSP with guidance from information owners, information security practitioners, information technology product developers, and organizations having extensive experience in defining and stating the principles of information security.

1.2 SCOPE

The GASSP Committee seeks the creation, maintenance, monitoring of, and adherence to the GASSP for information security in the broadest context, on an international level, unifying and expanding upon existing authoritative sources.

1.3 OBJECTIVES

☐ Identify and develop Pervasive, Broad Functional, and Detailed GASSP and protection profiles in a comprehensive framework of emergent principles, standards, conventions, and mechanisms that will preserve the availability, confidentiality, and integrity of information.
☐ Be an authoritative source for opinions, practices, and principles for information owners, information security practitioners, information technology products, and information systems.
☐ Define, implement, and subsequently operate under the governing GASSP infrastructure.
☐ Define and establish linkage to the Common Criteria Project.
☐ Maintain close liaison and coordination with other international authoritative bodies, that have developed related works, to establish and maintain GASSP based on these efforts.
☐ Define and establish liaison with bodies responsible for certifying professionals to encourage convergence.
☐ Promote broad awareness of information security and GASSP.
☐ GASSP will address management, user, and other interested parties' concerns at all levels to gain the broadest acceptance.

1.4 BACKGROUND

In 1990, the U.S. National Research Council published *Computers at Risk* (CAR),[1] a landmark book that emphasized the urgent need for the nation to focus attention on information security. The GASSP document is a direct result of recommendation number one from the CAR report (see Appendix A for CAR recommendation details).

Recommendation 1 — Promulgation of a comprehensive set of Generally Accepted System Security Principles, referred to originally as GSSP, that would provide a clear articulation of essential features, assurances, and practices.

The CAR report proposes the Generally Accepted Accounting Practices (GAAP) as a model for GASSP. It cites the Building Code and the Underwriter's Laboratory as examples of GASSP in other fields. It also recommends building on the experience captured by using the Trusted Computer System Evaluation Criteria (TCSEC), the Trusted Network Interpretation (TNI), and the Information Technology Security Evaluation Criteria (ITSEC) documents to create a broader set of criteria that will drive a more flexible process for evaluating single-vendor and conglomerate systems.

1.5 DEFINITION OF KEY TERMS

Generally Accepted

GASSP are conventional — that is, they become *generally accepted* by agreement (often tacit agreement) rather than formal derivation from a set of postulates or basic concepts. The principles have been developed on the basis of experience, reason, custom, usage, and, to a significant extent, practical necessity. The sources of established information security principles are generally the following:

☐ Pronouncements of an authoritative body (to be established), as appropriate, to establish information security principles.
☐ Pronouncements of bodies composed of expert information security practitioners that follow a due process procedure, including broad distribution of proposed information security principles for public comment, for the intended purpose of establishing information security principles or describing existing practices that are generally accepted. This includes information security audit guides and statements of position.

☐ Practices or pronouncements that are generally accepted because they represent prevalent practice in a particular industry or the knowledgeable application to specific circumstance of pronouncements. This includes interpretations and practices that are widely recognized and prevalent in the industry.
☐ Other information security literature including pronouncements of other professional associations or regulatory agencies and information security textbooks and articles.

The concept of generally accepted is to be distinguished from the concept of universally accepted. This distinction is made to address the case that all principles may have exceptions. For example, a library system may insist that the card catalog system have no accountability to preserve the privacy of the user. A process will be provided for use when it is deemed necessary to deviate from the published GASSP.

Generally Accepted System Security Principles (GASSP)

Generally Accepted System Security Principles incorporate the consensus, at a particular time, as to the principles, standards, conventions, and mechanisms that information security practitioners should employ, that information processing products should provide, and that information owners should acknowledge to ensure the security of information and information systems.

GASSP relates to physical, technical, and administrative information security and encompasses pervasive, broad functional, and detailed security principles. GASSP nomenclature considers the terms *policy*, *rules*, *procedures*, and *practices* to relate to the organizational implementation of security. Information technology (IT) changes rapidly, and GASSP are expected to evolve accordingly. Consensus regarding accepted information security principles is achieved first within the GASSP Committee followed by international IT community review.

Information

The term *information* applies to any storage, communication, or receipt of knowledge, such as fact, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.

Information System

The term *information system* describes the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

Information Security Principles

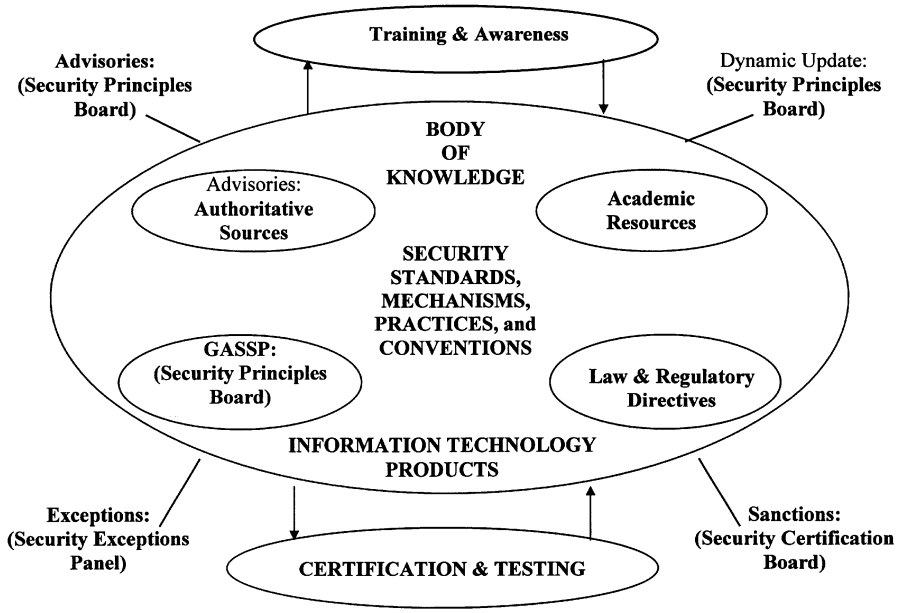
The term *information security principles* is used in its broadest context. It includes principles, standards, conventions, and mechanisms. Three categories (pervasive, broad functional, and detailed) are used to collect, discuss, and organize security principles. The broad functional and detailed security principles are divided into principles for information security practitioners and information processing products.

GASSP will support information security professional certification, information security audit, and information technology product development from an information security perspective. GASSP will also provide authoritative guidance to the information security practitioners, enabling them to establish and maintain their credibility with management.

System

The term *system* is used as an umbrella term for the hardware, software, physical, administrative, and organizational issues that need to be considered when addressing the security of an organization's information resources (see Exhibit 1). It implies that the GASSP address the broadest definition of information security. The term *system* is intended to be equivalent in scope of the terms *information technology* (IT), *automated information system* (AIS), *automated data processing element* (ADPE), etc.

EXHIBIT 1 Role of GASSP and Product Profiles in Relation to Information Systems Security Certification and the Body of Knowledge



2.0 PRINCIPLES

Candidate principles are organized in a three-level hierarchy. The hierarchy comprises:

☐ Pervasive Principles — few in number, fundamental in nature, and rarely changing.
☐ Broad Functional Principles — subordinate to one or more of the Pervasive Principles, are more numerous and specific, guide the development of more Detailed Principles, and change only when reflecting major developments in technology or other affecting issues.
☐ Detailed Principles — subordinate to one or more of the Broad Functional Principles, numerous, specific, emergent, and changing frequently as technology and other affecting issues evolve.

2.1 PERVASIVE PRINCIPLES

The Pervasive Principles address the following properties of information:

☐ Confidentiality
☐ Integrity
☐ Availability

The Pervasive Principles provide general guidance to establish and maintain the security of information. These principles form the basis of Broad Functional Principles and Detailed Principles. Security of information is achieved through the preservation of appropriate confidentiality, integrity, and availability. Confidentiality is the characteristic of information being disclosed only to authorized persons, entities, and processes at authorized times and in the authorized manner. Integrity is the characteristic of information being accurate and complete and the information systems' preservation of accuracy and completeness. Availability is the characteristic of information and supporting information systems being accessible and usable on a timely basis in the required manner.

The Pervasive Principles are founded on the Guidelines for Security of Information Systems, developed by the Information Computer and Communications Policy (ICCP) Committee and endorsed and published by the Organization for Economic Cooperation and Development (OECD).[2] See Appendix B.

The OECD principles have been interpreted and extended using the Authoritative Foundation, a list of fundamental works on information security compiled by the GASSP Committee to support the development of GASSP. See Appendix C.

Each Pervasive Principle is presented in the following format:

☐ GASSP Statement
☐ Rationale
☐ Example

2.1.1 Accountability Principle

Information security accountability and responsibility must be clearly defined and acknowledged.

Rationale. Accountability characterizes the ability to audit the actions of all parties and processes which interact with information. Roles and responsibilities are clearly defined, identified, and authorized at a level commensurate with the sensitivity and criticality of information. The relationship among all parties, processes, and information must be clearly defined, documented, and acknowledged by all parties. All parties must have responsibilities for which they are held accountable.

Example. Information assets should be controlled and monitored with an accompanying audit log to report any modification, addition, or deletion to the information assets. These logs should report the user or process that performed the actions.

2.1.2 Awareness Principle

All parties, including but not limited to information owners and information security practitioners, with a need to know should have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information.

Rationale. This principle applies between and within organizations. Awareness of information security principles, standards, conventions, and mechanisms enhances and enables controls and can help to mitigate threats. Awareness of threats and their significance also increases user acceptance of controls. Without user awareness of the necessity for particular controls, the users can pose a risk to information by ignoring, bypassing, or overcoming existing control mechanisms. The awareness principle applies to unauthorized and authorized parties.

Example. The security mechanism of wearing identification badges is weakened if not exhaustively enforced. If unidentified individuals go unchallenged, vulnerability is introduced to the system.

If every user, authorized or unauthorized, is made aware of the organization's position on unauthorized use and its potential consequences, e.g., via a logon banner, some misuse can be avoided.

2.1.3 Ethics Principle

Information should be used, and the administration of information security should be executed, in an ethical manner.

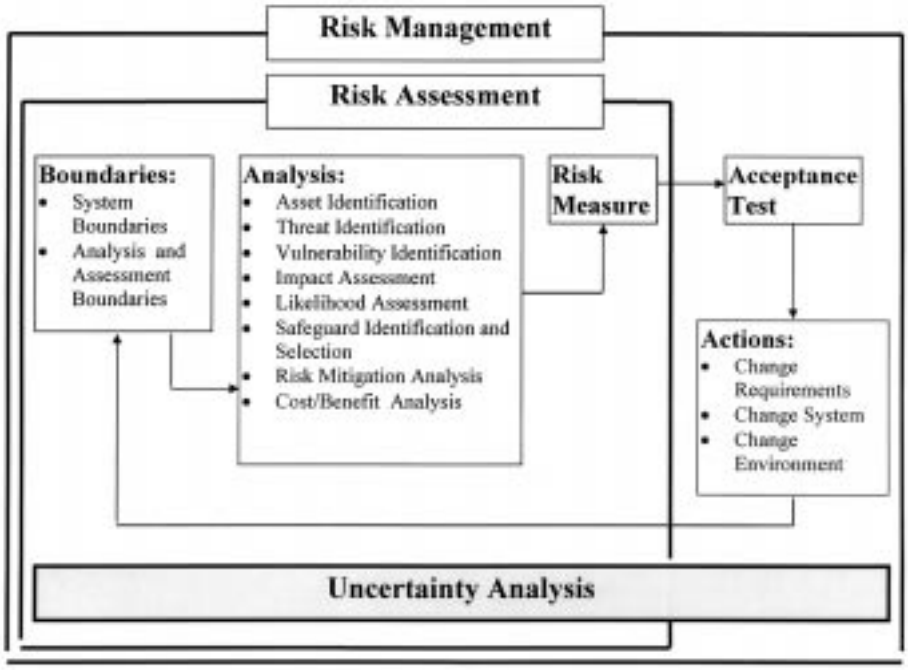
Rationale. Information systems pervade societies and cultures. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information. Use of information and information systems should match the expectations established by social norms, and obligations.

Example. Some organizations have developed a Code of Ethical Conduct that outlines for all employees a set of actions, behaviors, and conduct guidelines with respect to information security and information use. The code sets forth expectations for conduct that may not be illegal but may be contrary to an organization's policy or belief. Behavior outside the bounds of the code would be considered unethical.

2.1.4 Multidisciplinary Principle

Principles, standards, conventions, and mechanisms for the security of informa-

EXHIBIT 2 IT Security Risk Management Framework



tion and information systems should address the considerations and viewpoints of all interested parties.

Rationale. Information security is achieved by the combined efforts of information owners, users, custodians, and information security personnel. Decisions made with due consideration of all relevant viewpoints and technical capabilities can enhance information security and receive better acceptance.

Example. When developing contingency plans, organizations can establish a contingency planning team of representatives from facilities management, technology management, and other functional areas to identify better the various expectations and viewpoints from across the organization and other recognized parties.

2.1.5 Proportionality Principle

Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of the information.

Rationale. Security controls should be commensurate with the value of the information assets and the vulnerability. Consider the value, sensitivity and criticality of the information, and the probability, frequency, and severity of direct and indirect harm or loss. This principle recognizes the value of approaches to information security ranging from prevention to acceptance.

Example. Some organizations determine information security measures based on an examination of the risks, associated threats, vulnerabilities, loss exposure, and risk mitigation through cost/benefit analysis using a Risk Management Framework (see Exhibit 2).

Other organizations implement information security measures based on a prudent assessment of "due care" (such as the use of reasonable safeguards based on the practices of similar organizations), resource limitations, and priorities.

2.1.6 Integration Principle

Principles, standards, conventions, and mechanisms for the security of informa-

tion should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system.

Rationale. Many breaches of information security involve the compromise of more than one safeguard. The most effective control measures are components of an integrated system of controls. Information security is most efficient when planned, managed, and coordinated throughout the organization's system of controls and the life of the information.

Example. Accounts and accesses may be properly controlled when the information owner selects the right type and level of access for users, informs system managers of which users need accounts, and promptly informs them of changes. If one control in the system of controls is compromised, other controls can provide a safety net to limit or prevent the loss.

2.1.7 Timeliness Principle

All accountable parties should act in a timely, coordinated manner to prevent or respond to breaches of and threats to the security of information and information systems.

Rationale. Organizations should be capable of swift coordination and action to enable threat event prevention or mitigation. This principle recognizes the need for the public and private sectors to establish jointly mechanisms and procedures for rapid and effective threat event reporting and handling. Access to threat event history could support effective response to threat events and may help to prevent future incidents.

Example. An organization with access to timely threat and vulnerability information can make prompt decisions that will prevent or mitigate an incident. Expertise can be brought to bear on a problem, e.g., the introduction of a virus on an internal network, if it is rapidly reported to an organization's incident handling team.

2.1.8 Assessment Principle

The risks to information and information systems should be assessed periodically.

Rationale. Information and the requirements for its security vary over time. Risks to the information, to its value, and to the probability, frequency, and severity of direct and indirect harm/loss should undergo periodic assessment. Periodic assessment identifies and measures the variances from available and established security measures and controls, such as those articulated here in the GASSP, and the risk associated with such variances. Periodic assessment enables accountable parties to make informed, information risk management decisions whether to accept, mitigate, or transfer the identified risks with due consideration of cost effectiveness.

Example. Listed below are events that may trigger the need for a security assessment:

☐ a significant change to the information system
☐ a significant change in the information or its value
☐ a significant change in the technology
☐ a significant change to the threats or vulnerabilities
☐ a significant change to available safeguards
☐ a significant change in the user profiles
☐ a significant change in the potential loss of the system
☐ a significant change to the organization/enterprise
☐ a predetermined length of time since last assessment

2.1.9 Equity Principle

Management shall respect the rights and dignity of individuals when setting policy

EXHIBIT 3 Cross-Impact Matrix Relating BFPs to PPs

	PP-1	PP-2	PP-3	PP-4	PP-5	PP-6	PP-7	PP-8	PP-9
BFP-1	X	X	X	X	X	X	X	X	X
BFP-2	X	X	X	X					X
BFP-3	X	X	X	X					X
BFP-4	X	X		X				X	
BFP-5	X	X	X	X	X			X	
BFP-6	X	X		X					X
BFP-7	X			X	X	X	X	X	
BFP-8	X			X	X	X	X	X	
BFP-9	X			X	X	X	X	X	
BFP-10	X			X	X	X		X	
BFP-11	X	X		X	X	X	X	X	
BFP-12	X			X	X		X	X	
BFP-13	X	X	X	X					X
BFP-14		X	X	X					X

and when selecting, implementing, and enforcing security measures.

Rationale. Information security measures implemented by an organization should not infringe upon the obligations, rights, and needs of legitimate users, owners, and others affected by the information when exercised within the legitimate parameters of the mission objectives.

Example. Individual privacy should be protected. A system administrator may need access to private information for problem diagnosis and resolution only.

2.2 BROAD FUNCTIONAL PRINCIPLES

The Broad Functional Principles (BFP) are derived from the Pervasive Principles (PP) that represent the conceptual goals of information security. By providing the guidance for operational accomplishment of the Pervasive Principles, the Broad Functional Principles are the building blocks (what to do) that comprise the Pervasive Principles and allow definition of the basic units of those principles. Because the Broad Functional Principles are smaller in scope, they are easier to address in terms of implementation planning and execution.

Exhibit 3 presents the relationship of Broad Functional Principles to Pervasive Principles. Each Broad Functional Principle is presented in the following manner:

- ☐ BFP Title
- ☐ Statement of BFP
- ☐ Rationale
- ☐ Example

[Reference(s) to relevant "Control Objectives" from the ISACA CoBIT, the IIA SAC, the EU BS-7799, the OECD Information Security Principles, and other sources of safeguard guidance found in the GASSP Committee Foundation Document List (Appendix C).]

2.2.1 Information Security Policy

Management shall ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security. Such guidance must assign responsibility, the level of discretion, and how much risk each individual or organizational entity is authorized to assume.

Rationale. To assure that information assets are effectively and uniformly secured consistent with their value and associated risk factors, management must clearly articulate its security strategy and associated expectations. In the absence of this clarity, some resources will be undersecured — that is, ineffective; other resources will be oversecured — that is, inefficient.

It is essential that organizations establish, maintain, and promulgate a clearly articulated hierarchy of policies and supporting standards, baselines, procedures, and guidelines, including lines of authority and responsibility, that address the security of the information assets — and supporting Information Technology resources — the organization owns or for which it is responsible. These policies should reflect the mission statement of the owner of the information assets, as well as the value of the confidentiality, availability, and integrity of the information assets to the owner and other relevant parties. The policies must also reflect changes in the organizational mission statement as well as technology advances and other changes that could, if unrecognized or unaddressed, compromise the security of the information.

Development of a clearly articulated hierarchy of policies that address the security of an organization's information assets, or information assets for which it is responsible, assures that the owners, users, custodians, and information security personnel have clear guidance in effectively securing the information assets. Without the analysis and development of a clearly articulated hierarchy of policies addressing the security of its information assets, or information assets for which it is responsible, the owners, users, custodians, and information security personnel will not have clear guidance in assuring that information assets are effectively and efficiently secured. This lack of policy could result in the organization subjecting the information assets to undue risks and increasing the potential for unacceptable loss, liability, or harm to the organization and other relevant parties. Further, the lack of policy could result in the loss of management options for redress or remedy.

Example. Company ZYX developed procedures for system development, access control, and disaster recovery planning within the information technology department. These procedures, however, were not the result of management establishing sound policy. They were the result of IT management's perception that it should have documented procedures for some of the more complex activities. During routine system maintenance, "Jack Black," who was unhappy with his manager and the company, realized there was no prohibition of Trojan horses or other similarly malicious activity. Jack thus built a Trojan horse into a modification of the accounts receivable application system that he routinely maintained. He then submitted his resignation and left the company. Six months later, the Trojan horse, a logic bomb, began to corrupt files systematically on the birthday of his former manager. At first, this corruption appeared to be minor user errors and was ignored. But within a few weeks, the file was severely contaminated, as were all backup files. The result was a sustained inability to generate invoices and related accounts receivable.

The ability of ZYX to prosecute Jack was thwarted by the complete lack of policy articulating management and ownership perception of the value of the information assets. Jack was thus successful in his vengeful attack at great cost and embarrassment to ZYX.

2.2.2 Education and Awareness

Management shall communicate information security policy to all personnel and ensure that all are appropriately aware. Education shall include standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences of failure to comply.

Rationale. To ensure that all personnel are aware of security policy, management must effectively and regularly communicate its requirements. When personnel fail to do what management expects, it is more often the result of an ineffective or imperfect communication of what management expects, rather than the result of wrongful motive or intent on the part of the personnel. The failure to communicate regularly and effectively information security policy, standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and the consequences of failing to comply to all relevant parties can cause the unintentional breach of policy by parties to whom the policy has not been effectively communicated. Such failure can also result in the intentional breach of policy by parties to whom the adverse consequences of such a breach have not been effectively communicated.

In both cases, the potential for harm, liability, or loss to the organization or other relevant parties can be significant. The failure to communicate information security policy effectively can also impair the ability to apply enforcement measures, prosecute criminal activity, or seek civil redress successfully.

Example. ZYX Corp. decides to allow dial-up access to its Information Technology environment but fails to put a public notice on the logon screen advising all parties of its information security policy. Subsequently, an individual hostile to ZYX accessed the organization's information assets through the dial-up path and modified critical product formulae information, resulting in a substantial loss to the organization. In the civil litigation that followed, the court found in favor of the defendant, because there was no notice that the information was a valued asset and that unauthorized access was prohibited and would be prosecuted.

2.2.3 Accountability

Management shall hold all parties accountable for their access to and use of information, e.g., additions, modifications, copying and deletions, and supporting Information Technology resources. It must be possible to affix the date, time, and responsibility, to the level of an individual, for all significant events.

Rationale. To assure that people behave as expected, it is necessary to know who did what and when it was done.

It is essential that organizations establish and maintain a basis of control for information assets. Such a control framework requires individual and organizational accountability at all levels. The concept of "accountability" refers to the accepting of responsibility by all relevant parties or entities. Holding all parties thusly accountable is intended to assure that any use made of or actions taken on information assets and supporting Information Technology resources shall be for authorized "business/mission purposes only" and that such use or action can be reliably traced to the responsible party or parties, who will be held "accountable."

Example. When reviewing the daily access audit report, "Henry," the Information Security Officer (ISO), found several invalid Payroll file access attempts by "Edwina" in Personnel. When the ISO

spoke with her and her manager concerning this, it became obvious that she did in fact require access to the particular file. She was accordingly granted limited access. However, three other invalid attempts were found against the same file, and the owner of the userid was in the Graphic Arts Department. When the ISO spoke with "Jason" and his manager, it was determined that Jason was planning to ask for a raise, and his invalid accesses resulted from his attempt to learn what others in his department were being paid. Jason stated that, armed with such information, he would have an idea of what an acceptable pay increase might be. He would thus have an advantage in the raise negotiations. The ISO turned the matter over to Jason's manager for disciplinary action.

2.2.4 Information Management

Management shall routinely catalog and value information assets, and assign levels of sensitivity and criticality. Information, as an asset, must be uniquely identified and responsibility for it assigned.

Rationale. To manage information assets efficiently, management must know what to protect. To be effectively managed, it is essential to identify and enumerate the core attributes of information as assets. These information asset attributes include:

☐ identity
☐ ownership
☐ custody
☐ content
☐ value (ideally expressed in monetary terms) of the confidentiality, availability, and integrity of the information assets
☐ sensitivity (which relates directly to confidentiality)
☐ criticality (which relates directly to availability and integrity)

The organizational ownership of an information asset must be established. The person or agent/custodian legitimately established as the owner of an information asset has the authority and responsibility to make — or delegate — decisions regarding the security of the information asset. It is typically the organization that will ultimately suffer liability, loss, or other harm if the confidentiality, availability, or integrity of the information asset is compromised, although others may suffer harm or loss as well.

The identity and content of the information asset must be clearly established for the owner to make informed decisions regarding its security. Knowing the value of the information asset, as related to its confidentiality, availability, and integrity, enables the owner to understand the financial risks and associated threats that must be mitigated when establishing security requirements for the information asset.

Finally, these attributes should be reviewed regularly, because most information attributes change value over time — in some cases increasing and in others decreasing.

Example. XYZ, Inc., a Silicon Valley start-up with breakthrough technology, the Cyberwidget, established "Mr. Doe," vice president of Production, as the owner of its Materials Requirements Planning (MRP) systems. The MRP system included functions addressing inventory and shipping document production, and input to the Accounts Receivable invoicing process. Mr. Doe was already heavily tasked — and stressed — with meeting an increasing demand for the Cyberwidget. He repeatedly postponed meetings with the Information Security Officer (ISO) to discuss valuing the system and the supported information asset.

Because there was no financial case in place reflecting the value of the MRP system and supported information assets, management did not fund the previous year's ISO budget request for improved information security and contingency planning. In the following winter, a mudslide from a nearby hill swept into the information technology area dedicated to

production and destroyed much of the equipment. The production floor, however, suffered no direct impact.

The result was that the just-in-time (JIT) production process was interrupted, even though the production equipment was not damaged. Production was halted and finished production could not be shipped for weeks because the MRP, with inventory control, parts ordering and positioning, shipping documents, and supported invoicing process, was inoperable. Management panicked, the system recovery effort was severely impaired — there was no policy, recovery plan, or designation of responsibility — and clients canceled orders. Many clients reverted to proven vendors of similar, though less efficient, products. Consequently, the promising start-up company went into bankruptcy and never recovered.

2.2.5 Environmental Management

Management shall consider and compensate for the risks inherent to the internal and external physical environment where information assets and supporting Information Technology resources and assets are stored, transmitted, or used.

Rationale. To protect the organizational mission effectively, it is necessary to identify and address environmental threats that can disrupt Information Technology functionality. There are significant threats — and vulnerabilities — associated with the location, construction, and equipping of Information Technology facilities. These threats include:

☐ natural disaster threats (earthquake, flood, hurricane, tornado, landslides, etc.)
☐ unintentional or intentional physical threats (e.g., power outage, equipment failure, fire, proximity of potentially toxic or explosive industrial facilities and transportation infrastructures, local crime, and a wide array of accidents that could "exploit" unrecognized or inadequately addressed vulnerabilities of the physical environment)

For the optimum security strategy implementation, it is essential to coordinate and integrate information security efforts with overall organizational security measures and management. Failure to recognize and effectively address local threats and associated vulnerabilities, both internal and external, can result in a potentially disastrous disruption of Information Technology functionality.

Example. In the dead of winter, an organization impacted by natural disaster contacted its contracted Information Technology Disaster Recovery hot site provider, which offered a Disaster Recovery facility in the same geographic region. Just before the client's Information Technology recovery staff boarded an airplane to fly to the hot site, the roof of the facility collapsed from the weight of snow and ice on it. The hot site provider had not considered the ability of the facility roof to cope with the load of a major snow and ice accumulation. Thus, the hot site provider's building was not suitable to the mission, and no compensating provisions were made. Consequently, the hot site provider lost the client — and credibility — and had to rebuild the Disaster Recovery hot site. A competing provider quickly rescued the client.

2.2.6 Personnel Qualifications

Management shall establish and verify the qualifications related to integrity, need-to-know, and technical competence of all parties provided access to information assets or supporting Information Technology resources.

Rationale. To implement security effectively for information assets and supporting Information Technology resources, it is necessary that the personnel involved are competent with respect to the knowledge and technical skill needed to perform their roles reliably, that their integrity (as demonstrated by work history, academic and training certification, and references) meets organizational requirements, and

that their need-to-know is authoritatively established. Such personnel include, at a minimum:

☐ owners (as representatives of the organization and its interests)
☐ users
☐ contractors and supplemental staff
☐ custodians
☐ information security personnel

Example. "Joe B.," who represented himself as a CISSP, was hired by XYZ Corporation to develop and implement a corporatewide information security program. His first assignment was to conduct a risk assessment to determine the current state of information security in the corporation. After several weeks of effort, Joe submitted his report. Knowledgeable management, upon reviewing his report, noted that an obvious exposure was not documented in the report. XYZ Corporation had failed to implement policy and related standards, baselines, and procedures that would have addressed the prevention, detection, or containment of network attacks. Top management was advised of the risk to information assets and information processing confidentiality, integrity, and availability.

Subsequent investigation disclosed that Joe had not passed the CISSP examination and had not previously performed a risk assessment. Closer review of his report revealed numerous errors and misrepresentations. Joe was dismissed immediately, and personnel policy regarding the verification of credentials was augmented to assure that all qualifications upon which management relied to select staff were effectively validated.

Policy, standards, and procedures were then developed to ensure that appropriate countermeasures, safeguards, or controls were in place and used effectively to reduce risk to an acceptable level. Training sessions were provided to owners, custodians, and users to ensure that all concerned understood the need for and use of the countermeasures.

2.2.7 System Integrity

Management shall ensure that all properties of systems and applications that are essential to or relied upon to support the organization's mission are established, preserved, and safeguarded.

Rationale. For management to be able to rely upon the correct performance of Information Technology resources, it is necessary to ensure that they are implemented as intended and are not subsequently contaminated or corrupted by malicious acts, uncorrected error conditions, or other failures. Unless controls are in place to protect systems and applications from unauthorized modifications and to ensure that authorized changes are tracked and perform as intended, systems can fail in a way that impairs efficiency or even the health of the organization. Further, such failures may not be detected on a timely basis, because management assumes the integrity of the Information Technology resources.

Example. During month-end general ledger processing, the closing account levels for the Purchasing Department showed an unexpected surplus of cash. All subsidiary ledger, journal, and accrual accounts relating to Purchasing were then opened for additional verification and validation checking. During this review, it appeared that the Sales Tax Accrual and Posting ledger accounts were not as high as expected. When compared with earlier periods, it was found that accruals were substantially less (30 percent), given that activity levels were typically within 10 percent from one period to the next.

A final validation run was executed, and it was found that the cash surplus was the amount that should have been posted to the subsidiary ledger account with the entry of each purchase. All required adjusting entries were then performed, trial balances were calculated, and the results produced the correct balances in all related accounts.

A review was made to determine the cause of the errors. It was found that changes made to the Accounting System 33 days earlier produced the errors, due to the omission of critical internal control functions. The routines necessary to perform posting and validation performed correctly, but the account numbers used by the routines were invalid. Thus, the entries to be posted were retained in the original accounts, and, because no error checking was included in the changes, no error reporting output was generated to alert anyone to the problem.

The necessary internal control functions were subsequently reestablished, and the problem did not recur. Change control procedures were revisited and updated to prevent the omission of necessary control in the future.

2.2.8 Information Systems Life Cycle

Management shall ensure that security is addressed at all stages of the system life cycle.

Rationale. For management to be able to rely upon controls, they must be continuous. To be efficient, controls must be comprehensive and applied early. The security function must be fully integrated with system life cycle processes. Retrofit, repair, and other late remedies are always inefficient and may be ineffective. Late application of a control may be insufficient to restore a system to a desired or required robustness.

All in-place controls and countermeasures must be fully documented and periodically reviewed. For preproduction systems, phase reviews must assess intended security feature design, integration, and effectiveness. For in-production systems, maintenance phase reviews must be performed at every step to ensure consistent and correct performance, continued effectiveness and efficiency, accurate interface(s) with other applications, and the comprehensive maintenance of all contingency planning measures.

All reviews must be conducted in conformance with established guidelines that define minimum acceptable requirements for the effectiveness of controls in support of organizational standards for information confidentiality, system and data integrity, and the availability of the information asset and supporting Information Technology resources.

Example. Operating System (OS) maintenance was planned for the Engineering Design Control Section system. It was known that the system held planning data for all new plant designs, including details of proprietary processes, specifications of valve prototypes under consideration for inclusion, and other highly confidential data. The systems administrator knew from his analysis that three modules of the OS would be overwritten by new versions. He expressed concern that the in-place modules would revert to the original installation parameters, thus erasing all file access rules and potentially exposing sensitive data to users having no authority to access the information. The maintenance team agreed to test this concern in an isolated but identically configured environment before conversion.

During the test procedure, the maintenance team found that the system administrator's concerns were well founded — the file access rules were indeed erased. The team found a solution, which was to make archival copies of the rules database, perform the conversion, then lay in the rules database following conversion. Extensive testing in the isolated environment proved that this option performed correctly, and the system maintenance subsequently proceeded successfully.

2.2.9 Access Control

Management shall establish appropriate controls to balance access to information assets and supporting Information Technology resources against the risk.

Rationale. To achieve a level of risk mitigation commensurate with the value of the information asset to be secured, access

to information assets and supporting Information Technology resources should be restricted to the smallest population consistent with other business needs, based on the criteria of a clearly delineated "need-to-know." Through this standard, the information systems-dependent workforce is facilitated in the accomplishment of assigned tasks by ensuring that all required information is available only through appropriately controlled means. Specifically, individual employees and other parties are restricted from access to information assets and supporting Information Technology resources that do not directly relate to their work requirements, assigned objectives, or legitimate, authorized need.

By enforcing such a standard, the owner or custodian limits the exposure of potentially sensitive information assets and supporting Information Technology resources and enables management to assert appropriate control over the access to, modification of, or the dissemination of sensitive information assets in terms of content and recipient. Therefore, potentially adverse consequences resulting from uncontrolled access or distribution are minimized.

Example. "Diane Thomas," Director of Benefits and Compensation for XYZ, Inc., was reviewing salary plans from all departments, and found that proposed salary increases for the next fiscal year were 15 percent higher than had been discussed at a budgetary planning meeting earlier that year. She met with the compensation manager to discuss the unexpected figures before returning them to the department managers to be reworked. Dave questioned the figures and where the department managers got their justification. The manager responded that the justification used was the forecasted 25 percent increase in company revenues over last year. Probing further, Diane asked where that information was obtained and was told it was available online from the accounting system. Diane ended the meeting and went to see "Jay Brock," Director of Finance.

After hearing the situation, Jay became very concerned that confidential budget forecast information seemed to be freely available instead of being limited to directors and senior corporate officers. Diane requested that "Maurice McDonnell," the Director of Information Systems, join them immediately. When Maurice arrived, and the situation was explained to him, he promptly left to look into it. Maurice called his System Security Officer (SSO) in and asked for a report on the access control rules for the accounting system. Two hours later, the SSO returned with the report, and, in reviewing it, they found no rule in place for the file containing the forecast information.

To remedy this, Maurice called Jay, and they agreed to take the file off-line until an appropriate rule could be put in place. Thus, future inappropriate access was prevented, and what could have been the costly disclosure of highly sensitive strategic information was limited to the discovery of an embarrassing lapse in access control management.

2.2.10 Operational Continuity and Contingency Planning

Management shall plan for and operate Information Technology in such a way as to preserve the continuity of organizational operations.

Rationale. To protect information assets and supporting Information Technology resources from disruptive events, or to be able to rapidly restore their proper functioning in the case that such a disruptive event is unavoidable, it is essential that organizations establish a cohesive set of preventive, mitigative, and restorative measures, as determined to be appropriate and cost-effective by risk assessment.

Organizational entities depend on their Information Technology resource infrastructure now more than at any previous time in history to deliver mission-critical

information in a timely fashion. The operational importance of information assets, whether based on cost or time factors, is such that organizations can ill afford to endure the consequences of significantly disruptive events impacting supporting Information Technology resources or the information assets directly.

Example. A risk assessment performed at XYZ, Inc., showed that the ground-floor Central Computing Services Complex (CCSC) was well isolated from most major disruptive agents, except for flooding. The executive in charge of Information Technology stated that when the ten-story structure was built, area flooding had occurred no more recently than 15 years ago, and all steps then believed appropriate to mitigate this threat were taken. The systems security officer, "John W.," CISSP, pointed out that in the intervening period, additional construction had occurred, but no corresponding flood control measures had been taken. Additionally, Joe mentioned that weather statistics showed that each year the tropical storm count increased, as had the attendant rainfall amounts, with the result that larger amounts of water pooled for longer periods in places where they had not 15 years earlier.

It was generally recognized that a flood would damage or destroy the Information Technology facilities on the first floor. Historically, flood cleanup had required four to six weeks in this area. Also, a service outage of greater than 14 days would render XYZ, Inc., financially insolvent. When asked for recommendations, Joe stated that the XYZ flood insurance must be reviewed to ensure that it is commensurate with asset values and corporate requirements as they currently stand.

Joe further recommended that management consider relocating the CCSC to a higher floor in the building, or away from the current building, where the threat of flooding could be reduced or eliminated. When questioned concerning the cost of these and other measures, Joe stated that the most costly recommendation was less than $700K, while the estimated cost to clean up the facility and replace all damaged equipment in the event of total loss exceeded $15M. He further stated that an appropriate increase in flood insurance would add less than 0.5 percent to the insurance expense line of the corporate operational budget.

2.2.11 Information Risk Management

Management shall ensure that information security measures are appropriate to the value of the assets and the threats to which they are vulnerable.

Rationale. To choose effective and efficient information security measures, management must identify the assets to be protected, the threats to the assets, and the vulnerability of the assets or their environment to the threats.

The security of information assets, with regard to the value of their confidentiality, integrity, and availability, and the security of the supporting Information Technology resources must be assured by well-informed owners, managers, custodians, or other responsible parties. Such an approach (performed strategically, on an ongoing basis, or as changes dictate) must enable well-informed decisions regarding whether to accept, mitigate, or transfer the risks associated with the information assets and supporting Information Technology resources. These decisions should be based on the monetary value of the assets, probability and consequences of direct or indirect harm or loss, related threats, effectiveness of existing safeguards and controls, and whether additional safeguards or controls could be expected to provide cost-effective incremental risk mitigation.

Example. In migrating to a newer version of the standard corporate e-mail, a team of analysts working for ABC, Inc., assessed whether or not the in-place access rules would migrate intact. This was regarded as

a critical factor, since highly confidential project information was passed regularly from one department head to another. In the post-migration test analysis, the team found that proxy rules did not transfer, with the result that mail became visible to the "public." Also found was a failure of the encryption feature, due to version incompatibilities, when applied to mail sent externally.

The directors of internal audit and corporate legal reviewed the matter for potential ramifications. Given the kind of information that could have been compromised, their consensus was that exposure to loss of intellectual property, and possible violation of employee privacy, could have exposed the company to an estimated $39M in total losses; $9M of loss would stem from a combination of litigation costs and settlements in privacy matters, and another $30M from redevelopment costs due to exposure of proprietary process details while in transit to remote corporate sites. Consequently, the transition effort was halted until the problem was fully resolved and effective security measures were implemented and successfully tested.

2.2.12 Network and Infrastructure Security

Management shall consider the potential impact on the shared global infrastructure, e.g., the Internet, public-switched networks, and other connected systems when establishing network security measures.

Rationale. To compensate for the increased vulnerability from and to things outside of the organization, as created by connection to systems beyond the organization, the threat and risk model must be changed to reflect the threat from and to things outside the organization. For example, connecting a UNIX system to the public switched network puts the UNIX system at risk, and connecting the UNIX system to the Internet puts other systems at risk.

All methods for accessing Information Technology resource connectivity must contain controls and countermeasures that implement the established security policy of the organization appropriate to the sensitivity or criticality level of the Information Technology resources and supported information assets. Such controls must, at a minimum, reflect the same security level as the information itself to ensure consistency and cohesiveness of overall policy implementation. This consideration must extend to the physical as well as the logical aspect of the connectivity.

The potential to subvert access to the Information Technology resources and supported information assets is greatest in terms of connectivity through persistent connections, but increases with temporary connections. This same potential exists, however, through in-house networks, although these are inherently less flexible in their vulnerability to exploitation. Therefore, the security implementation must first identify the specific weaknesses in each access method and the potential consequences of their exploitation. Then each weakness can be addressed through the application of measures intended to achieve a level of protection commensurate with the sensitivity/criticality of the Information Technology resource and the supported information assets.

Example. Having received the first request for dial-in access, "Joe A." carefully assessed the stated need and the description of the resources required. The national sales manager carried a laptop and required access from several company locations throughout the country, some of which had no in-house computer access. The data he would transmit was going to be sales volumes and dollar amounts, both considered very confidential. Joe knew that strong security steps would be required to meet this unique situation.

Looking at several options, Joe selected a combination of SmartCard, encryption, and callback measures to secure the dial access port link. The callback would confirm physical location (linked to a tele-

phone line with no "Call-Forward" feature), encryption would provide data confidentiality, and the SmartCard facility would serve to provide user identification and authentication. Given that the database that the national sales manager would access had its own built-in userid and password routine, Joe believed that together these measures would provide proper security.

2.2.13 Legal, Regulatory, and Contractual Requirements of Information Security

Management shall take steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets.

Rationale. For an organization to comply diligently with all legal, regulatory, and contractual requirements associated with its operations, it is necessary to ensure that no requirement exists for which compliance measures have not been put in place. As part of this effort, plans should also be in place to address potential actions against the organization should their policy, processes, or actions be called into question.

Example. During the final review of XYZ Company's Statement of Work for its Department of Energy (DoE) contract prior to "Best-and-Final" submission, it was noted by the director of engineering that no provisions had been included specifically regarding protection of information assets belonging to the government. There was only general text that reflected awareness of the confidential nature of the work. This prompted a review of the contract to determine what specifications addressed this topic, and what the potential liability of XYZ would be by leaving unaddressed any such specifications. The review showed that penalties of up to $10,000 per day would accrue for failure to comply with stated performance requirements. Additionally, until compliance was reestablished, the contractor would forfeit all accrued performance awards.

A contract review meeting was called, and the contracting officers, along with DoE personnel, discussed information asset protection requirements. Subsequent to the meeting, the Statement of Work was amended to address the stated specifications. It was determined that had XYZ failed to address this matter from the inception of the contract, a four-month period would have been required to initiate and complete compliance efforts. This would have resulted in a loss of $120K in penalties, $500K in accrued performance awards, and compliance effort costs of $110K when performed after contract inception. The cost added to the contract to perform the work from inception was, by comparison, estimated to be less than $60K.

2.2.14 Ethical Practices

Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.

Rationale. To preserve employee morale and the perception of the organization and its management as fair and ethical, and recognizing that security measures may be or become unduly intrusive, management must be candid, fair, and conservative in developing and enforcing security policy.

Management must carefully consider employee privacy. The key to successful policy is strict observance of fairness and respect for the individual. No policy is complete proof against culpability, but careful construction and consistently unbiased execution contribute positively to the organization's overall risk management program.

Policy provisions, including consequences for noncompliance, must be understandable and enforceable, and enforcement must be fairly applied. Candor helps ensure fairness. Security mea-

sures that cannot be disclosed should not be applied.

Owner's conservative rule: Owners should assume that others would treat their assets as belonging to the public domain. Therefore, they should explicitly declare (in reasonably visible ways) the products of their efforts and their property to be either private or public.

User's conservative rule: Assume that any tangible or intangible item belongs to somebody else unless an explicit declaration or convention identifies it as being in the public domain or authorized for your use.

Example. BCA Corp. hired "Jim Blue" to implement and manage its logical access control policy. Jim promptly found that many userids and passwords belonging to terminated employees were still active, although their owners were gone, some for several years. He also found that one of these userid/password combinations had been used subsequent to the owner's departure. Files accessed included confidential personnel and payroll records of a key executive. Although no one had noticed, the executive's files had been altered to imply that a medical condition had become a significant risk. This fabricated medical problem could have affected the executive's career upon his next review, given the high stress nature of his job.

Assuming that the departed party had violated the company's privacy policy, Jim wrote a letter to the executive accusing the former employee of a breach of privacy. The executive was outraged. An investigation ensued, the police were consulted, and the individual accused was interrogated aggressively. In addition, Jim, feeling guilty for having made his accusation perhaps prematurely, carefully reviewed logical access management procedures and practices applied prior to Jim's being hired. The investigation revealed that the management of logical access controls had previously been so poor that a significant number of employees could have executed the inappropriate modification, and determining who was responsible was impossible.

The unethical action of accusing the former employee prior to establishing the facts resulted in substantial embarrassment to the company, which avoided a potentially costly lawsuit only by promptly offering a generous settlement.

2.3 DETAILED SECURITY PRINCIPLES

The Detailed Security Principles specifically address methods of achieving compliance with the Broad Functional Principles with respect to existing environments and available technology. There will be many detailed information security principles supporting one or more Broad Functional Principles. The Detailed Principles will address differing technologies, environments, standards, practices, and concepts that are relevant to the Broad Functional Principles. The Detailed Principles are expected to evolve continuously to meet the challenges of emerging technology and new threats.

Following is an example of a Detailed Principle (and its underlying rationale) supporting a Broad Functional Principle (Access Control), which supports the Pervasive Principle (Proportionality):

> Use one-time passwords to control logical access to all information assets deemed critical to an organization.
>
> Multiple-use passwords were originally the only technique available to control access to a system. Changes in technology made the multiple-use password obsolete in many environments. Therefore, the one-time password evolved. Future technological advances will probably result in the use of smart card technology, replacing current password technology. (There will be separate Detailed Principles that expand upon and guide the application security mechanisms in the users' environment.)

3.0 REFERENCES

1. National Research Council, Dr. David Clark (MIT), committee chair, *Computers at Risk,* National Academy Press, 1991.
2. Organization for Economic Cooperation and Development (OECD), *Guidelines for the Security of Information Systems,* 1992.

3.1 BIBLIOGRAPHY

An Introduction to Computer Security: The NIST Handbook (Draft), National Institute of Standards and Technology, 1994.

Nathan Bisk, Jr., CPA Comprehensive Exam Review: Auditing, 1985.

GASSP Committee Project Plan Draft 3.0, GASSP Committee, September 1994.

Glossary of Computer Security Terminology, NIST IR 4659, National Institute of Standards and Technology, September 1991.

M. E. Kabay, "Social Psychology and INFOSEC: Psychosocial Factors in the Implementation of Information Security Policy."

Robin Moses, Ian Glover, and Len Watts, "Updated Framework for Computer/Communications Security Risk Management," from *Proceedings of the 3rd International Computer Security Risk Management Model Builders' Workshop,* sponsored by Los Alamos National Laboratory, NIST, and MSCS, 1990.

Ali Mosleh, "A Framework for Computer Security Risk Management," from *Proceedings of the 3rd International Computer Security Risk Management Model Builders' Workshop,* sponsored by Los Alamos National Laboratory, NIST, and NCSC, 1989.

Donn Parker, "Information Security for Applications in Distributed Computing," from the *Proceedings for the Second AIS Security Technology for Space Operations Conference* (NASA/JSC Mission Operations Directorate and the Texas Gulf Coast Chapter of the ISSA cosponsors), 1993.

Micki Krause and Harold F. Tipton, Eds., *Information Security Management Handbook,* Auerbach Publications, Boca Raton, FL, 2000.

Charles Cressen Wood, *Information Integrity: Principles of Secure Information Systems Design,* Elsevier Science, New York, 1990.

Appendix A: Guidance from Computers at Risk

Major recommendations from *Computers at Risk* that are addressed by GASSP:

1. Promulgation of a comprehensive set of Generally Accepted System Security Principles, referred to as GASSP, which would provide a clear articulation of essential features, assurances, and practices.
2. A set of short-term actions for system vendors and users that build on readily available capabilities and would yield immediate benefits.
3. Directions for a comprehensive program of research.
4. Establishment of a new organization to nurture the development, commercialization, and proper use of trust technology, referred to as the Information Security Foundation, or ISF.

Specific guidance from CAR for recommendation 1 and others related to GASSP is as follows:

1. Promulgate comprehensive Generally Accepted System Security Principles (GASSP).
   a. Establish a set of GASSP for computer systems.
   b. Consider the system requirements specified by the Orange Book for the C2 and B1 levels as a short-term definition of GASSP and a starting point for more extensive definitions.
   c. Establish methods, guidelines, and facilities for evaluation of products for conformance to GASSP.
   d. Use GASSP as a basis for resolving differences between U.S. and foreign criteria for trustworthy systems and as a vehicle for shaping inputs to international discussions of security and safety standards.
2. Take specific short-term actions that build on readily available capabilities.
   a. Develop security policies.
   b. Use as a first step the Orange Book's C2 and B1 criteria.
   c. Use sound methodology and modern technology to develop high-quality software.
   d. Implement emerging security standards and participate actively in their design.
3. Establish an Information Security Foundation to address needs that are not likely to be met adequately by existing entities.
   a. Establishment of GASSP.
   b. Research on computer system security, including evaluation techniques.
   c. System evaluation.
   d. Brokering and enhancing communications between commercial and national security interests.
   e. Focused participation in international standardization and harmonization efforts for commercial security practice.

Appendix B: Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems

Paris 1992

PREFACE

Explosive growth in the use of information systems for all manner of applications in all parts of life has made provision of proper security essential. Security of information systems is an international matter because the information systems themselves often cross national boundaries and the issues to which they give rise may most effectively be resolved by international consultation and cooperation.

In 1990, the Information, Computer and Communications Policy (ICCP) Committee created a Group of Experts to prepare Guidelines for the Security of Information Systems. The Group of Experts included governmental delegates, scholars in the fields of law, mathematics, and computer science, and representatives of the private sector, including computer and communication goods and services providers and users. The Expert Group was chaired by the Hon. Michael Kirby, President of the Court of Appeals, Supreme Court of New South Wales, Australia. Ms. Deborah Hurley of the Information, Computer and Communications Policy Division of the OECD Directorate for Science, Technology and Industry drafted the Recommendation, the Guidelines, and the Explanatory Memorandum, based upon the deliberations of the Expert Group at its meetings.

The Expert Group met six times over 20 months — in January 1991, March 1991, September 1991, January 1992, June 1992, and September 1992 — to prepare the Recommendation of the Council Concerning Guidelines for the Security of Information Systems, the Guidelines for the Security of Information Systems, and the Explanatory Memorandum to Accompany the Guidelines. The Group of Experts submitted the final version of the three texts to the ICCP Committee at its 22nd session on 14–15 October 1992. The ICCP Committee approved the texts and their transmission to the Council of the OECD.

On 26 November 1992, the Council of the OECD adopted the Recommendation of the Council Concerning Guidelines for the Security of Information Systems and the 24 OECD Member countries adopted the Guidelines for the Security of Information Systems.

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS 26 NOVEMBER 1992

THE COUNCIL, HAVING REGARD TO:

the Convention on the Organization for Economic Cooperation and Development

of 14 December 1960, in particular, articles 1 (b), 1 (c), 3 (a), and 5 (b) thereof;

the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [C(85)139, Annex].

RECOGNIZING:

the increasing use and value of computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance (all hereinafter referred to collectively as "information systems");

the international nature of information systems and their worldwide proliferation; that the increasingly significant role of information systems and growing dependence on them in national and international economies and trade and in social, cultural, and political life call for special efforts to foster confidence in information systems;

that, in the absence of appropriate safeguards, data and information in information systems acquire a distinct sensitivity and vulnerability, as compared with paper documents, due to risks arising from available means of unauthorized access, use, misappropriation, alteration, and destruction;

the need to raise awareness of risks to information systems and of the safeguards available to meet those risks;

that present measures, practices, procedures, and institutions may not adequately meet the challenges posed by information systems and the concomitant need for rights and obligations, of enforcement of rights, and of recourse and redress for violation of rights relating to information systems and the security of information systems;

the desirability of greater international coordination and cooperation in meeting the challenges posed by information systems, the potential detrimental effects of a lack of coordination and cooperation on national and international economies and trade and on participation in social, cultural, and political life, and the common interest in promoting the security of information systems;

AND FURTHER RECOGNIZING:

that the Guidelines do not affect the sovereign rights of national governments in respect of national security and public order ("order public"), subject always to the requirements of national law; that, in the particular case of federal countries, the observance of the Guidelines may be affected by the division of powers in the federation;

RECOMMENDS THAT MEMBER COUNTRIES:

1. establish measures, practices, and procedures to reflect the principles concerning the security of information systems set forth in the Guidelines contained in the Annex to the Recommendation, which is an integral part hereof;
2. consult, coordinate, and cooperate in the implementation of the Guidelines, including international collaboration to develop compatible standards, measures, practices, and procedures for the security of information systems;
3. agree as expeditiously as possible on specific initiatives for the application of the Guidelines;
4. disseminate extensively the principles contained in the Guidelines;
5. review the Guidelines every five years with a view to improving international cooperation on issues relating to the security of information systems.

Annex to the Recommendation of the Council of 26 November 1992

GUIDELINE FOR THE SECURITY OF INFORMATION SYSTEMS 26 NOVEMBER 1992

I. Aims

The Guidelines are intended:

☐ to raise awareness of risks to information systems and of the safeguards available to meet those risks;
☐ to create a general framework to assist those responsible, in the public and private sectors, for the development and implementation of coherent measures, practices, and procedures for the security of information systems;
☐ to promote cooperation between the public and private sectors in the development and implementation of such measures, practices, and procedures;
☐ to foster confidence in information systems and the manner in which they are provided and used;
☐ to facilitate development and use of information systems, nationally and internationally, and
☐ to promote international cooperation in achieving security of information systems

II. Scope

The Guidelines are addressed to the public and private sectors.
The Guidelines apply to all information systems.
The Guidelines are capable of being supplemented by additional practices and procedures for the provision of the security of information systems.

III. Definitions

For the purposes of these Guidelines:

☐ *data* means a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human beings or by automatic means
☐ *information* is the meaning assigned to data by means of conventions applied to that data
☐ *information systems* means computers, communication facilities, computer and communication networks, and data and information that may be stored, processed, retrieved, or transmitted by them, including programs, specifications, and procedures for their operation, use, and maintenance
☐ *availability* means the characteristic of data, information, and information systems being accessible and usable on a timely basis in the required manner
☐ *confidentiality* means the characteristic of data and information being disclosed only to authorized persons, entities, and processes at authorized times and in the authorized manner
☐ *integrity* means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness

IV. Security Objective

The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.

V. Principles

1. Accountability Principle

The responsibilities and accountability of owners, providers, and users of information systems and other parties concerned with the security of information systems should be explicit.

2. Awareness Principle

To foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices, and procedures for the security of information systems.

3. Ethics Principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary Principle

Measures, practices, and procedures for the security of information systems should take account of and address all relevant consider-

ations and viewpoints, including technical, administrative, organizational, operational, commercial, educational, and legal.

5. Proportionality Principle
Security levels, costs, measures, practices, and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability, and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

6. Integration Principle
Measures, practices, and procedures for the security of information systems should be coordinated and integrated with each other and with other measures, practices, and procedures of the organization so as to create a coherent system of security.

7. Timeliness Principle
Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.

8. Reassessment Principle
The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Equity Principle
The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

VI. Implementation

Governments, the public sector, and the private sector should take steps to protect information systems and to provide for their security in accordance with the Principles of the Guidelines. In achieving the Security Objective and in implementing the Principles, they are urged, as appropriate, to establish and to encourage and support the establishment of legal, administrative self-regulatory, and other measures, practices, procedures, and institutions for the security of information systems. Where provision has not already been made, they should, in particular:

Policy Development
☐ Adopt and encourage the adoption of appropriate policies, laws, decrees, rules, and international agreements, including provision for:
- – harmonized worldwide technical standards, methods, and codes of practice
- – promotion of expertise and best practice in the security of information systems
- – formation and validity of contracts and other documents created and executed in or by means of information systems
- – allocation of risks and liability for failures of the security of information systems
- – penal, administrative, or other sanctions for misuse of information systems
- – jurisdictional competence of courts, including rules on extraterritorial jurisdiction, and administrative competence of other bodies
- – mutual assistance, extradition, and other international cooperation in matters relating to the security of information systems
- – means of obtaining evidence in information systems and the admissibility of such evidence in penal and nonpenal legal and administrative proceedings

Education and Training
☐ Promote awareness of the necessity for and the goals of security of information systems, including:
- – ethical conduct in the use of information systems
- – adoption of good security practices

☐ Provide and foster education and training of:
- – developers, owners, providers, and users of information systems
- – specialists and auditors of information systems

– specialists and auditors of security of information systems
– law enforcement authorities, investigators, attorneys and judges

Enforcement and Redress

☐ Provide accessible and adequate means for the exercise and enforcement of rights arising from the implementation of the Guidelines and for recourse and redress for violations of those rights.

☐ Provide prompt assistance in procedural and investigative matters relating to breaches of security of information systems.

Exchange of Information

☐ Facilitate the exchange of information relating to the Guidelines and their implementation.

☐ Publish generally measures, practices, and procedures established in observance of the Guidelines and for the security of information systems.

Cooperation

☐ On national and international levels, consult, coordinate, and cooperate between and among governments and the private sector to encourage implementation of the Guidelines and to harmonize as completely as possible measures, practices, and procedures for the security of information systems.

EXPLANATORY MEMORANDUM

to Accompany the Guidelines for the Security of Information Systems

Preface

In October 1988, the Committee for Information, Computer and Communications Policy (ICCP) of the OECD approved the preparation by the OECD Secretariat of a study on the subject of security of information systems. The report, entitled Information Network Security, was submitted to the ICCP Committee in October 1989. Following review of the Secretariat document, the ICCP Committee endorsed the convocation of a meeting of experts to explore in greater depth the issues raised in the report.

Based upon the advice of the experts, the ICCP Committee, in March 1990, approved the creation of a Group of Experts to draft Guidelines for the Security of Information Systems. The Group of Experts included governmental delegates, scholars in the fields of law, mathematics, and computer science, and representatives of the private sector, including computer and communication goods and services providers and users. The Group of Experts met six times between January 1991 and September 1992 to prepare the Recommendation of the Council concerning Guidelines for the Security of Information Systems, the Guidelines for the Security of Information Systems, and the Explanatory Memorandum to Accompany the Guidelines.

The OECD is well-positioned to play a central role in building awareness of the need for security of information systems and of measures that might be undertaken to meet that end. OECD membership encompasses North America, the Pacific region, and Europe. The lion's share of development and exploitation of information systems occurs in OECD member countries. Through the ICCP Committee, the OECD provides direction and coalesces opinion at an early stage on issues related to information, computer and communication technologies and policies, and their effects on society, with a view to raising awareness on an international level and assisting governments and the private sector as they undertake national deliberations.

The Guidelines for the Security of Information Systems are intended to provide a foundation upon which countries and the private sector, acting singly and in concert, may construct a framework for security of information systems. The framework will include laws, codes of conduct, technical measures, management and user practices, and public education and awareness activities; it is hoped that

the Guidelines will serve as a benchmark against which governments, the public sector, the private sector, and society may measure their progress.

Introduction

A computer, a computer program, and data constitute basic elements of an information system. The computer may be connected by communication equipment and devices into a network with terminals or other computers or communication facilities. A network may be a private local area network (LAN), an extended private network, such as a wide area network (WAN) or global network, or an external communication link open to anyone with the technological means to gain access to it. Many networks are composed of a combination of internal and external links. Communication networks include data communication, telephone, and facsimile. Other ancillary equipment, printers, for example, may be attached to the computer and communications hardware. The computer programs might include operation system and application software, which may be custom-designed or purchased ready-made. The software, may be installed in the computer or stored on magnetic, optical, or other media. Paper manuals and documentation support the operation, use, and maintenance of the hardware and software. This entire structure is created for the purpose of storing, processing, retrieving, and transmitting data and information. These various elements may be combined to form an information system.

Expanding Uses and Benefits of Information Systems

The significance of computer and communications technologies, economically, socially, and politically, is widely accepted. They are key technologies not only in their own right but also as conduits for and components of other goods, services, and activities.

Recent years have witnessed:

☐ proliferation of computers
☐ increase of computing power with simultaneous decrease in costs
☐ convergence of computer and communication technologies
☐ greater interconnectivity and interoperability of computer and communication systems
☐ increasing decentralization of computing and communication functions and
☐ growth of computer use to the point that, in many countries, every individual is an actual or potential user of computer and communication networks

The global information society has arrived. It is borderless, unconstrained by distance or time. Economies, politics, and societies are based less on geography and physical infrastructure than previously, and more on information system infrastructures.

Information systems benefit governments, international organizations, private enterprise, and individuals. They have become integral to national and international security, trade, and financial activity. They are widely used by government administrations, fiscal authorities, business organizations, and research institutions. They are critical to the provision of health care, energy transport, and communications. Information systems may be used for trading, voting, learning, and leisure. Expanded use of information systems offers possibilities of greater access to resources, experience, learning, and participation in cultural and civic life.

Dependency

Every person, enterprise, and government is affected by information systems and has become dependent on their continued proper functioning. For example, increased use of information systems has wrought fundamental changes in internal systems has wrought fundamental changes in internal organizational procedures and has altered the way that organizations interact. In the event of an information system failure, it may be neither possible to continue present procedures without

information systems nor practicable to return to former methods. There may not be sufficient paper records, staff skills, or even numbers of staff to permit an organization to continue to work as productively as it does with its information system in operation, and as effectively as its competitors. Consider, for example, the effect of information system failure on the functioning and efficiency of airlines, banks, or securities exchanges.

Dependence on information systems is growing. Concomitant is a mounting need for confidence that the systems will continue to be available and to operate in the expected manner.

Vulnerability

As use of information systems has increased enormously, generating many benefits, it has, in its wake, created an ever-larger gap between the need to protect systems and the degree of protection utilized at present. Society, including business, public services, and individuals, has become very dependent on technologies that are not yet sufficiently dependable. All the uses of information systems identified above are vulnerable to attacks upon or failures of information systems. There are risks of loss from unauthorized access, use, misappropriation, modification, or destruction of information systems, which may be caused accidentally or result from purposeful activity. Certain information systems, both public and private, such as those used in military or defense installations, nuclear power plants, hospitals, transport systems, and securities exchanges, offer fertile ground for antisocial behavior or terrorism.

The developments identified above, proliferation of computers, increased computing power, interconnectivity, decentralization, growth of networks and the numbers of users, while enhancing the utility of information systems, also increase system vulnerability. It may be harder to locate a system problem and its causes, to correct it in balance with other system functions and requirements, and to prevent its recurrence or the occurrence of other lapses. As systems decentralize and grow larger, it is important to keep account of their interdependent components, which, increasingly, may come from multiple vendors and sources. Moreover, the growing interconnectivity of network systems and use of external networks multiply points of possible information system failures. These externalities lie outside the direct control of the system operators and the rights and duties of the parties in the event of breaches may be unclear.

Technical change is uneven. It leaps ahead in some areas while lagging in others. Inability to adapt to and absorb technological developments at the same rate at which they occur, such as failure to test or coordinate system changes adequately, may lead to system problems. Technological developments may be implemented before all their ramifications and relations to existing technologies are understood. Unequal distribution of system capabilities may give some persons more control of and access to information systems than is intended or desirable. Increasing numbers of users have access to information systems, while, at the same time, system owners or providers decreasingly control them directly.

Failures of information systems may result in direct financial loss, such as loss of orders or payment, or in losses that are more indirect or perhaps less quantifiable by, for example, disclosure of information that is personal, important to national security, of competitive value, or otherwise sensitive or confidential.

The evolution of the law is not always in step with technological progress. It is sometimes insufficient at the national level and in a number of cases still undeveloped at the international level. Harmonization of legislation is an important goal to be actively pursued.

Building Confidence

Users must have confidence that information systems will operate as intended with-

out unanticipated failures or problems. Otherwise, the systems and their underlying technologies may not be exploited to the extent possible and further growth and innovation may be inhibited. Access to secure networks and establishment of security standards has already emerged as general user requirements. Loss of confidence may stem equally from outright malfunction or from functioning that does not meet expectations.

Uncertainties may be met and confidence fostered by building consensus about the use of information systems. Accepted procedures and rules are needed to provide conditions to increase the reliability of information systems. Developers, operators, and users of information systems deserve reassurance regarding their rights and obligations, including responsibility for system failures. Clear, uniform, predictable rules should be in place to ease and encourage growth and exploitation of information systems.

The security of information systems is an international issue because information systems and the ability to use them frequently cross national boundaries. It is a problem that may be ameliorated by international cooperation. Indeed, given the disregard of information systems for geographic and jurisdictional boundaries, agreements are best promulgated and accepted on an international level.

Experience in other sectors involving new technologies with the potential for serious harm reveals a three-part challenge: developing and implementing the technology; providing for avoiding and meeting the failures of the technology; and gaining public support and approval of use of the technology. The air transport industry has been fairly successful in implementing safety techniques and requirements. It facilitates the smooth functioning of air transport and inspires public confidence. Similarly, the shipping industry has successfully used ship certification systems to rank the safety of vessels. The field of biotechnology is now grappling to meet the requirements of permitting technological development and preventing harm from exploitation of the technology and subsequent loss of public support. For information and communication technologies, the goal of avoiding and meeting failures of the technology includes the additional task of preventing and handling actual or potential intrusion to information systems.

Security of Information Systems

Security of information systems is the protection of availability, confidentiality, and integrity. Information systems have the attribute "availability" if they are accessible and usable on a timely basis and in the required manner. Confidentiality is the characteristic of data and information being disclosed only to authorized persons, entities, and processes at authorized times and in the authorized manner. Integrity is the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness. The relative priority and significance of availability, confidentiality, and integrity vary according to the information system.

Threats to Information Systems

Technological development, technical problems, extreme environmental events, adverse physical plant conditions, human institutions, all present challenges to the smooth functioning of information systems. Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. They range from cataclysmic events to minor, daily inefficiencies. Downtimes, for example, may be caused by a large breakdown or by frequent slow-ups or service degradations. The frequency and duration of disturbances, however minor, should be considered when planning for security. Large and small events may be equally disruptive to system functioning and use and may be equally debilitating to the organization's effective operation.

Technical factors leading to failures of information systems are numerous, sometimes not well understood, and constantly changing. They may be computer and communications hardware or software faults and malfunctions, caused by bugs, overloads, or other operational or quality problems. The difficulty may arise in an internal system component (system collection of computer system or a distributed system; application and operating system software, such as a compiler or editor; LANs), an external system component (telecommunication circuits, satellites) or from the interaction of different parts of the system.

Technical problems may be caused by intentional attacks on the system. Viruses, often introduced into the system via infected software, parasites, trap doors, Trojan horses, worms, and logic bombs are some of the technical means used to disrupt, distort, or destroy normal system functions.

The difficulty of providing security for networks and information is compounded in multiple-vendor environments. For example, a significant problem is the availability of access-control software, a commonly used security measure, that is compatible with the entire system in a multiple-vendor environment. To facilitate development of effective security for information systems, standards bodies, governments, and vendors and users of information systems must agree on standards for security measures.

Physical threats to information systems fall into two broad categories: extreme environmental events and adverse physical plant conditions. Extreme environmental events include earthquake, fire, flood, electrical storms, and excessive heat and humidity. The information system may be housed in a building, in which, in addition to computers and communication lines located throughout the building, there may be dedicated computer rooms and data storage rooms. Connections for power supply and communication may lead to and from the building. Adverse physical plant conditions may arise from breach of physical security measures, power failures or surges, air conditioning malfunction, water leaks, static electricity, and dust. An organization may be affected by lapses either directly at its premises or indirectly at a vital point outside the organization, such as power supply or telecommunication channels.

Human beings and the institutions they establish to reflect their values, whether social, economic, or political, as well as the lack of such institutions, all contribute to security problems. The diversity of system users — employees, consultants, customers, competitors, or the general public — and their various levels of awareness, training, and interest compound the potential difficulties of providing security.

Lack of training and follow-up about security and its importance perpetuate ignorance about proper use of information systems. Without proper training, operators and users may not be aware of the potential for harm from system misuse. Poor security practice abounds. Operators and users may not take even the most rudimentary security measures.

The choice of a password, a nearly universal user activity and usually a user's first activity on a system, provides a striking example. Although passwords are employed to control access to most information systems, few users are instructed on the need for password security, on the manner in which to create a password, or on penalties for misuse of the system. Without guidance, many users choose obvious passwords that may be easily ascertained, such as family or pet names, joke words, or words related to the task. After logging in to the system, untrained users may leave active terminals connected to network systems unattended, display passwords on the side of terminals, fail to create backup data files, share user identification codes and passwords, and leave open access-control doors into high-security areas. These are threshold security

problems that arise from entering a room, switching on a computer or terminal, possessing a password, and logging in.

Errors and omissions may occur in gathering, creating, processing, storing, transmitting, and deleting data and information. Failure to back up critical files and software multiplies the negative effects of errors and omissions. If files have not been backed up, the organization may incur significant expense in time and money in recreating them.

Intentional misuse of authorized system access and unauthorized system access ("hacking") for the purposes of mischief, vandalism, sabotage, fraud, or theft are additional serious threats to system and organizational viability. Unauthorized copying of software (software piracy), for example, is widespread. Popular conception holds that the greater part of threats to information systems comes from external sources. On the contrary, persons who have been granted authorized access to the system may pose a larger threat to information systems. They may be honest, well-intentioned employees who, because of fatigue, inadequate training, or negligence, commit an inadvertent act that deletes massive amounts of data. They may be disgruntled or dishonest employees who misuse or exceed authorized access to tamper deliberately with the system for their own enrichment or to the detriment of the organization.

Computer programs are an important element of information systems and a potentially fertile terrain for threats to information systems. A program containing a virus that is introduced into an information system may affect the availability, confidentiality, and integrity of that system by overloading the system, changing the list of authorized users of certain parts of the system, or altering data or information in the system. Violations of provisions of licensing agreements relating to the information system (e.g., software licensing agreements, database licensing agreements) may pose an additional security threat. Unauthorized alteration of the licensed program, for example, may trigger malfunctions as the modified software interacts with other parts of the system. Disclosure of proprietary information may damage an organization's competitive position.

Proper procedures must extend beyond the computer terminal and communication lines to the entire information arena. Improper handling of data and information storage media (whether paper, magnetic, or other) and improper handling and disposal of discarded computer printouts may lead to security breaches. Computer printouts may contain proprietary or competitive information or clues regarding system access. Yet, many companies have no policy for their disposal. Once used for the organization's purpose, they are considered worthless and discarded along with the day's used envelopes and pencil shavings. There may, however, be no expectation of privacy in trash, at least in trash that is outside the premises.

Insufficient use of systems may also lead to security problems, such as maintaining information availability or integrity in the event of shortages of qualified personnel, whether as a result of employees changing jobs, the introduction of new technologies requiring new skill, or work slowdowns, stoppages, or strikes.

Social, political, and economic institutions have not kept pace with technological development and growth in use of information systems. The price is uncertainty and lack of uniformity, which increase expense, cause delays, and, if permitted to continue, might impede future growth. There is a glaring deficiency of codes of practice, standards, and legal guidance and apportionment of legal rights and obligations.

Harm Resulting from Security Failures

Security failures may result in direct and consequential losses. Direct losses are those to the hardware, including processors, workstations, printers, disks and tapes, and communication equipment; the software,

including systems and applications software for central and remote devices; the documentation, including specifications, user manuals, and operation procedures; the personnel, including operators, users, and managerial, technical, and support staff; and the physical environment, including computer rooms, communications rooms, air conditioning and power supply equipment. Although direct losses may account for a small percentage of total losses arising from a security failure, nonetheless, the absolute investment in developing and operating the system will usually have been significant. The system requires protection in its own right as the container and channel for the data and information. The need to protect the system and the manner of doing so are inextricably linked to protecting the data and information that the system stores, processes, and transmits in order both to preserve the availability, confidentiality, and integrity of the data and information and to prevent alteration or damage of the container and channel through introduction of data and information, such as viruses, that may have a deleterious effect on operation and use of the system.

A consequential loss may occur when an information system fails to perform as intended. Consequential losses resulting from security failures may include loss of goods, other tangible assets, funds, or intellectual property; loss of valuable information; loss of competitive advantage; reduction in cash flow; loss of orders business; loss of production efficiency, effectiveness, or safety; loss of customer or supplier goodwill; penalties from violation of statutory obligations; and public embarrassment and loss of business credibility. Consequential losses account for most of the losses arising from security lapses. In light of that fact, protection against consequential loss, which, above all, means protecting the data and information, must be a top priority.

Enhancing Security

The goals of confidentiality, integrity, and availability must be balanced both against other organizational priorities, such as cost-efficiency, and against the negative consequences of security breaches. The cost must not exceed the benefit. Similarly, from the viewpoint of deterring those who would attempt to enter information systems to view, manipulate, or obtain information, security controls should be sufficient to render the costs or the amount of time required greater than the possible value to be gained from the intrusion.

Adequate measures for security of information systems help to ensure the smooth functioning of information systems. In addition to the commercial and social benefits of information systems already mentioned, security of information systems may assist in the protection of personal data and privacy and of intellectual property in information systems. Similarly, protection of personal data and privacy and of intellectual property may serve to enhance the security of the information system.

The use of information systems to collect, store, and cross-reference personal data has increased the need to protect such systems from unauthorized access and use. Methods to protect information systems include user verification or authentication, file access control, terminal controls, and network monitoring. Such measures generally contribute both to the security of information systems and to the protection of personal data and privacy. It is possible that certain measures adopted for the security of information systems might be misused so to violate the privacy of individuals. For example, an individual using the system might be monitored for a non-security-related purpose or information about the user made available through the user verification process might permit computerized linking of the user's financial, employment, medical, and other personal data. The principles of the Guidelines (for example, the Proportionality Principle and the Ethics Principle) and those of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

give guidance in achieving compatible realization of the goals of security of information systems and protection of personal data and privacy.

Information systems may include hardware, computer programs, databases, layout designs for semiconductor chips, data, and information, elements of which may be protected by intellectual and industrial property laws. Intellectual property in information systems is intangible, may cross borders virtually imperceptibly, and may be vulnerable to theft by the effort of one finger in a matter of seconds without taking the original and without leaving a trace. Security of information systems may reinforce the protection of intellectual property by limiting unauthorized access to components of the system, such as software or competitive information.

Since contracts, transactions, and disputes relating to information systems may involve parties, actions, and evidence in many different jurisdictions, it may be useful to clarify existing rules or presumptions or to establish new ones with regard to the law applicable in matters relating to the security of information systems. Given that disputes related to the security of information systems may involve complex factual situations as well as parties, actions, and evidence that may be situated in multiple jurisdictions, it may also be advisable to develop nonjudicial means, including arbitration, for resolution of disputes.

Guidelines for the Security of Information Systems

Aims

This section of the Guidelines sets forth the purposes to be served by their formulation and adoption by governments and the private sector. The Guidelines are intended to assist the further development and use of information systems. To do so, it is viewed as necessary to raise awareness of risks to information systems and to provide reassurance of the reliability of information systems and their provision and use. In recognition of the ubiquity of information systems, governments and the private sector are urged to cooperate to create an international framework for security of information systems. It is hoped that the Guidelines will contribute to increasing awareness of the importance of security of information systems and to dispelling reluctance to report security breaches, which might permit the compilation of more national and international statistics.

Scope

The Guidelines are intended to apply to all information systems, whether owned, operated, or used by public or private entities or for public or private purposes. The information systems may be of a public or private nature and elements of them may be protected by intellectual property or industrial property laws or other laws (e.g., trade secrets, official secrets). The Guidelines are not intended to supersede or otherwise affect the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The objective of the Guidelines is to avoid the evolution of a dual approach, one for information systems related to national security and one for all other information systems. Notwithstanding these intentions, it is fully accepted that governments may find it necessary to depart from the Guidelines. This is the case in the areas of national security and maintenance of public order ("order public"). The fact that governments have the sovereign right to what they must in these vital areas is recognized in the Recommendation of the Council Concerning Guidelines for the Security of Information Systems. However, it is expected that any departure from the Guidelines will relate more to the section on implementation than to the nine principles. The general idea is that exceptions to the Guidelines would be few and, since they relate to "sovereign" matters, would be of the highest order of importance. Furthermore, it was foreseen that appropriate information relating to departures from

the Guidelines, whether involving a public or private information system, would generally be made known to the public and all interested parties.

Definitions

The definition of information systems includes computer hardware; interconnected peripheral equipment; software, firmware, and other means of expressing computer programs; algorithms and other specifications either embedded within or accessed by such computer programs; manuals and documentation on paper, magnetic, optical, and other media; communication facilities, such as terminal/customer premises equipment and multiplexers, on the information system side or the network termination point of public telecommunication transport networks as well as equipment for private telecommunication networks not offered to the public generally; security control parameters; storage, processing, retrieval, transmission, and communication data, such as check digits and packet switching codes and procedures; data and information about parties accessing information systems; and user identification and verification measures (whether knowledge based, token based, biometric, behavioral, or other). This definition may include elements that are proprietary or nonproprietary, public or private. This definition applies to elements whether or not they interact with the data being transmitted by the system or are necessary for the operation, use, and maintenance of the other components of the system.

Confidentiality and integrity apply to *data* and *information*. The words data and information are repeated in the definition of availability, even though the term *information systems* includes them, to emphasize that availability also covers data and information. Confidentiality, integrity, and availability may be important for reasons of competitive advantage, national security, or to fulfill legal, regulatory, or ethical obligations, such as fiduciary duties, protection of personal data and privacy or medical confidentiality. Examples of availability are up-time and response time of the information system.

Security Objective

The Principles of the Guidelines, which follow the Security Objective, express essential concepts to be considered in protecting information systems and providing for their security. The Principles are preceded by a simple declaration of the purpose and goals of security of information systems. Security of information systems is the protection of availability, confidentiality, and integrity. In the absence of sufficient security, information systems and, more generally, information and communication technologies may not be used to their full potentials. Lack of security or lack of confidence in the security of information systems may act as a brake on information system development and use and on development and use of new information and communication technologies. One goal, therefore, is the protection of individuals and organizations from harm resulting from failures of security. All individuals and organizations potentially rely on the proper functioning of information systems. Clear examples are the information systems in hospitals, air traffic control systems, and nuclear power plants. Security, therefore, is directed at preserving the effectiveness of information systems. In addition to the goal of ensuring that the level of availability, confidentiality, and integrity of information systems is not eroded, the security of information systems and the Guidelines are directed toward facilitating the development and use of information systems by individuals and for new and different purposes than those for which they are at present employed, as well as toward facilitating the development and exploitation of information and communication technologies.

Principles

The Guidelines identify nine principles in connection with security of information systems. They are the Accountability Prin-

ciple; the Awareness Principle; the Ethics Principle; the Multidisciplinary Principle; the Proportionality Principle; the Integration Principle; the Timeliness Principle; the Reassessment Principle; and the Equity Principle.

Accountability Principle. There should be an express and timely apportionment of responsibilities and accountability with respect to the security of information systems among owners, providers, and users of information systems and others. The phrase "other parties concerned with the security of information systems" includes executive management, programmers, maintenance providers, information system managers (software managers, operations managers, and network managers), software development managers, managers charged with security of information systems, and internal and external information system auditors.

Awareness Principle. This principle is meant to assist those with a legitimate interest to learn of or be informed about security of an information system. It is not intended as an opening to gain access to the information system or specific security measures and should not be construed as tending to jeopardize security. The level of information sought pursuant to this principle should be able to be obtained without compromising security.

Owners and providers are included in the Awareness Principle for there may be circumstances in which they, too, may need to acquire information about the security of a system. For example, an owner of a network may enter into an agreement whereby another organization would use the network to provide services for third parties. The owner may require, as part of the agreement, the certain levels of security be offered or available. In this circumstance, the owner may wish to be able to be informed of the security of the information system. Similarly, and organization that contracts with a computer or network owner to provide services may desire assurances regarding security and the ability independently to verify security. Users are also included in the Awareness Principle. For example, a customer choosing a bank may have a legitimate interest in being generally informed about the existence of security policies and programs of various banks. Depending upon customer demand, security might even come to be used as a marketing tool.

Ethics Principle. Information systems pervade societies and cultures. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information systems. This principle supports the development of social norms in these areas. Important aspects are the expression of these norms to all members of society and inculcation of these concepts from a very young age.

Multidisciplinary Principle. When devising and maintaining measures, practices, and procedures for the security of information systems, it is important to review the full spectrum of security needs and available security options. In an organization, for example, this would involve consultation with technical personnel, management, the legal department, users, and others. All these resources that should be consulted and combined to produce an optimal level of security for the information system. Similarly, on a policy level, technical standards, codes of practice, legislation, public awareness, education, and training for security of information systems may be mutually reinforcing.

From another aspect, this principle acknowledges that information systems may be used for very different purposes and that the security requirements may vary as a result. For example, the civil and military branches of government may have dissimilar needs for security as may different types of businesses or the commercial sector and private individuals.

Proportionality Principle. Every information system does not require maximum security. As it is important that systems not be insufficiently secure, so is it futile to provide security beyond the reasonable requirements of the system? Rather, there is a hierarchy of information systems and their security needs that differs for each organization. For this reason, there is no one security solution.

In assessing security needs, the information should first be identified and a value assigned. Possible security measures, practices, and procedures available to protect the various elements of the information system should be enumerated and the costs of implementing and maintaining each of the security options calculated. The level and type of security should then be weighed against the severity and probability of harm and its costs as well as the cost of the security measures. This analysis should be carried out for the information system in the context of all other relevant procedures and systems, including other information systems.

Integration Principle. Security of information systems is best considered when the system is being designed. Measures for security may be formulated and tested to avoid incompatibility. Overall costs of security may also be reduced. Security is required at all phases of the information cycle — gathering, creating, processing, storing, transmitting, and deleting. Security is only as good as the weakest link in the system.

Timeliness Principle. In the environment of the interconnected information systems that span the globe, the importance of time and place are diminished. It is possible to gain access to information systems regardless of physical location. The Timeliness Principle acknowledges that, due to the interconnected and transborder nature of information systems and the potential for damage to systems to occur rapidly, parties may need to act together swiftly to meet challenges to the security of information systems. Depending upon the security breach, the relevant parties may be members of the public and private sectors and may be located in different countries or jurisdictions. This principle recognizes the need for the public and private sectors to establish mechanisms and procedures for rapid and effective cooperation in response to serious security breaches.

Reassessment Principle. This principle recognizes that information systems are dynamic. System technology and users, the data and information in the system, and, accordingly, the security requirements of the system are ever-changing. The information systems, their value, and the severity, probability, and extent of potential harm should, therefore, undergo periodic reassessment. Follow-up is as important as implementation, especially in light of new technological developments, whether those adopted by the system owner on those available for use by others.

Equity Principle. The security interests of owners, developers, operators, and users of information systems must be weighed against the legitimate interests in the use and flow of information with the aim of striking a balance in accordance with the principles of a democratic society. Those unfamiliar with security of information systems may presuppose that security of information systems may lead only to restrictions to access to and movement of data and information. On the contrary, security may enhance access and flow of data and information by providing more accurate, reliable, and available systems. For example, harmonization of technical security standards will help to prevent data and information islands and other barriers to data and information flows.

Implementation

National governments should strive to ensure that territorial subdivisions in their countries are aware of the Guidelines and their implications for areas within the competence of the subdivisions. They

should communicate at the political level to all territorial subdivisions the text of the Guidelines, undertake every effort to urge their implementation, and consult regarding difficulties that may arise.

Self-regulation may take the form of codes of conduct or practice developed and adopted by individual organizations, industry, or professional associations or public sector agencies.

Policy Development: Worldwide Harmonization of Standards. There is a need for creation of appropriate technical security standards (including product and system evaluation criteria) with the widest possible geographic range of applicability. Their development should be the product of collaboration between, among others, governments, standards bodies, and vendors and users of information systems.

While seeking harmonized standards, it should be recalled that, as to individual situations, there can be no one security solution. Security needs vary considerably from sector to sector, company to company, department to department, and, as to given information systems, over time. Lack of an informed and balanced understanding of users' needs may create a significant risk of "off-target" technology standardization. A productive first step is recognition of the inherent diversity and heterogeneity of users' needs for information system safeguards.

Promotion of Expertise and Best Practice. Governments, public sector agencies, industry and professional associations and organizations should work together to promote expertise and to develop and promote awareness of concepts of "best practice" in the field of security of information systems. This may include notions of risk analysis, risk management, insurance, or audits. The particular program adopted may vary from organization to organization and from sector to sector. The security requirements of the banking sector, for example, may differ from those of other sectors.

Contract Formation and Validity. The goals of parties to an electronic transaction are not very different from those in a paper transaction. Generally, the participants in an information transfer, whether electronic or nonelectronic, want to know that the information came from the person who purports to have sent it, that it is received only by persons intended to receive it, and that it arrived in the intended form, unaltered and unmanipulated. Although the goals of parties to electronic and nonelectronic transactions may be basically the same, the manners of achieving these aims are not. They differ as a function of the means of creation, use, transmission, storage, and access to electronic and nonelectronic information. The manners in which the two types of information are protected perforce differ as well.

The challenge is to bring to electronic dealings the same level of confidence that at present exists for paper transactions. This may be accomplished in several ways. First, existing rules may be applicable to electronic situations. As necessary, existing rules may be modified and new ones developed. Technological means may also be employed. Further study and refinement of commercial laws involving electronic transactions might be useful, including rules relating to the validity of electronic signatures, the formation and validity of contracts created and executed in information systems, and enforcement of and liability for such contracts.

Allocation of Risks and Liability. There seems to be a dearth of rules relating to allocation of risks and liability for damage arising from security lapses. The relevant parties may include vendors, distributors, telecommunication operators, service providers, and users. Several systems may be involved in an information transfer, often including systems outside the ownership of control of the information processor or transmitter. The rights and duties of the parties involved may be unclear in cases of

mistakes, omissions, failures of the various systems or other mishaps.

The need for such rules exists and is illustrated when funds that are electronically transferred between two financial institutions are lost or stolen. Such transfers may involve vast amounts of money, are common financial practice, and are made almost instantaneously and across international boundaries. Where existing rules are not sufficient, further development and refinement on the national and international levels on the manner in which to assign liability in cases of fraudulent or negligent wire transfers is supported.

Sanctions. Sanctions for misuse of information systems are an important means to protect the interests of those relying on information systems from harm resulting from attacks to the availability, confidentiality and integrity of information systems and their components. Examples of such attacks include damaging or disrupting information systems by inserting viruses and worms, alteration of data, illegal access to data, computer fraud or forgery, and unauthorized reproduction of computer programs. In combating such dangers, countries have chosen to describe and respond to the offending acts in a variety of ways. There is growing international agreement on the core of computer-related offenses that should be covered by national penal laws. This is reflected in the development of computer crime and data protection legislation in OECD member countries during the last two decades and in the work of the OECD and other international bodies on legislation to combat computer-related crime. National legislation should be reviewed periodically to ensure that it adequately meets the dangers arising from the misuse of information systems.

At the same time, it is recognized that many factors may aggravate or mitigate the seriousness of the conduct: the specific intent of the actor, the type of data affected (e.g., national security or medical data), the extent of the harm, and the extent to which the actor exceeded authorization. For minor violations, the use of administrative sanctions, such as the imposition of nonpenal fines by an administrative agency, is considered by some nations (especially in the area of data protection) to be sufficient. Other types of sanctions may include, for example, disciplinary measures against civil servants or civil sanctions.

The development of legislation in OECD member countries has already led, particularly under the influence of international organizations, including the OECD, to a certain degree of harmonization. To further international cooperation in penal matters (including in the areas of mutual assistance, extradition and other international cooperation described below), this harmonization process should be supported and taken into account by countries when reviewing their legislation.

Jurisdictional Competence. In addition to the jurisdictional competence of courts in matters relating to the security of information systems, some countries may wish to grant certain administrative agencies rights to impose administrative sanctions.

The transborder character of data flow on the one hand and the mobility of offenders on the other hand may create problems in prosecuting computer criminals. Ideally, there should be harmonized rules on extraterritorial jurisdiction. However, pending the development of such rules, individual countries should review the suitability of their domestic jurisdictional rules to deal with transborder offenses. In countries where the doctrine of ubiquity (a crime is committed where one of its elements takes place) is not acknowledged, difficulties arise as to the application of national computer crime laws. In such countries, it may be necessary to introduce special jurisdictional rules, as, for instance, was done in the United Kingdom, where the Computer Misuse Act 1990 claims jurisdiction when

the hacker or computer is in the United Kingdom or where the interference makes use of a computer in the United Kingdom.

If a national of a state commits a computer-related crime in another state, problems may also arise when the crime is detected and the perpetrator is in the home country. Many countries do not extradite nationals. In such situations, an extension of the existing rules of extraterritorial jurisdiction (or the possibility of transfer of proceedings (see the following paragraph) should be considered with a view to creating the necessary prerequisites for a successful prosecution in at least one state.

Mutual Assistance and Extradition. Mutual assistance agreements, extradition laws, recognition and reciprocity provision, transfer of proceedings, and other international cooperation in matters relating to the security of information systems may facilitate assistance to other countries in their investigations.

Evidence. Improved security of information systems, by enhancing the accuracy, completeness, and availability of data and information in the information system and, accordingly, by increasing the ability to rely on data and information in the system, may assist the introduction and use of such evidence in legal and administrative proceedings. Similarly, in legal systems with special formal requirements regarding evidence, clear rules of evidence in both penal and civil legal and administrative proceedings may make information systems more secure by providing more predictability in actions involving failures or breaches of security and by the potentially deterrent effect of such actions.

At present, electronic records may present problems for existing laws of evidence. For European continental countries, which have civil law systems, the admissibility of evidence in court is based upon the principle of free introduction and free evaluation of evidence. This is also the situation in Japan with respect to nonpenal matters. In theory, under such legal systems, a court may admit any material as evidence, including computer records, but it must then decide the value such material will be afforded as evidence.

In common law countries, however, the admissibility of evidence is subject to objection and governed by complex rules. Computer records, like any other documents, may present two issues. The first is authentication: Are the documents accurate and genuine? Are the printouts from the computer admissible either as "originals" or "copies" of the data in the system? In the United States, for example, the federal rules expressly allow authentication and admission of computer records. The second issue that common law systems must address with respect to any document is whether or not it contains hearsay. This pertains not to the form of the document (whether electronic data or handwritten) but to its content. Generally, it is possible to testify only about matters of which one has direct knowledge and not about something learned from secondary sources. This rule applies to documents as well as to individuals and, while the hearsay rule has many exceptions (the business records rule, for example), this issue must be recognized and anticipated.

Education and Training. An overarching task is the increase of awareness at every level of society, in governments and the private sector and among individuals, of the necessity for and the goals of security of information systems and good security practices. Promotion of awareness should also include awareness of the risks to information systems and of safeguards available to meet those risks. It is important to develop social consensus about proper use of information systems.

In building awareness, it is essential to have the cooperation of users of information systems and the commitment of man-

agement, especially senior management, to providing for security of information systems.

Education and training should be included in school curricula and should be provided for users, executive management, programmers, maintenance providers, information system managers (software managers, operations managers, and network managers), software development managers, managers charged with security of information systems, and auditors of information systems and of security of information systems, both internal and independent auditors. Trained, professionally qualified auditors should inspect and evaluate an information system. Information system auditors should possess knowledge of planning, development, and operation of information systems and of general auditing and should have actual experience in performing information system audits. It is equally important that law enforcement authorities, including police and investigators, and attorneys and judges receive adequate education and training.

Enforcement and Redress. There should be provided accessible and adequate means for exercise and enforcement of rights related to the security of information systems and for recourse and redress of violations of such rights. This includes access to courts and provision of means for adequate investigative powers. Security breaches include failures and violations of security of information systems. There is a need for better cross-education, communication, cooperation, and sharing of information among law enforcement agencies, communications operators and service providers, and banks at national and international levels. Law enforcement authorities should cooperate to facilitate investigations in other countries.

Exchange of Information. Governments, the public sector, and the private sector should exchange information and establish procedures to facilitate the exchange of information relating to the Guidelines and their implementation. As part of their efforts, they should publish generally measures, practices, and procedures established in observance of the Guidelines and for the security of information systems. It is desirable that national governments make known to the OECD, other international bodies, and other governments their activities and those of their territorial subdivisions relating to the security of information systems, the Guidelines, and their implementation.

Cooperation. Governments, the public sector, and the private sector should develop measures, practices, and procedures that are simple and compatible with those of other parties that comply with the Guidelines taking into consideration in their development the measures, practices, and procedures developed by others, so to avoid, where possible, conflicts or obstacles. All laws adopted on regional, national, or provincial levels should be harmonized to meet the challenges of a worldwide technology.

Appendix C: GASSP Committee Foundation Document List

FOUNDATION DOCUMENT LIST (INCLUSIVE TO DATE) (DRAFT, 6/13/94)

The list is arranged alphabetically by contributing organization with individual documents shown numerically. Each document includes line items for title, publishing organization, individual author, and a brief description, where appropriate.

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTS

1. *Statements of the Accounting Principles Board* — Copyright 1993, Chapter 6, Generally Accepted Accounting Principles (GAAP) — Pervasive Principles American Institute of Certified Public Accountants, Inc. (AICPA)

BELLCORE, BELL COMMUNICATIONS

1. *Bellcore Operations Systems Security Requirements* — Issue 1, 6/91 Bellcore, Bell Communications Research Technical Advisory TA-STS-001194
2. *Bellcore Standard Operating Environment Security Requirements* — Issue 2, 6/91, Bellcore

DEPARTMENT OF TRADE AND INDUSTRY (DTI)

1. *A Code of Practice for Information Security Management* — Copyright 1993 Department of Trade and Industry (DTI) Commercial IT Security Group with Business Standards Institution (BSI)
2. *The U.K. IT Security Evaluation and Certification Scheme* — 10/92 The Department of Trade and Industry (DTI) for Enterprise
3. *User Requirements for IT Security Standards* — Crown copyright 1992, U.K. Department of Trade and Industry (DTI) with BSI/DISC in association with the Sema Group

COMMISSION OF THE EUROPEAN COMMUNITIES (SOG-IS)

1. *Green Book on the Security of Information Systems* — Draft 3.7, 10/5/93 (Replaces 2.6 of 7/14/93) Commission of the European Communities, Senior Officials Group — Information Security (SOG-IS)
2. *Information Technology Security Evaluation Criteria (ITSEC)* — Provisional Harmonized Criteria — 6/92 Commission of the European Communities, Senior Officials Group, Information Security (SOG-IS)
3. *Information Technology Security Evaluation Manual (ITSEM)* — V.1.0, 9/10/93 (replaces V.0.2, 4/92) Commission of the European Communities, DG XIII/B/B6
4. *Joint Workplan for EC/US Cooperation on Security of Information Systems* — DG XIII/F, 1, 2/27/92 Senior Officials Group, Information Security (SOG-IS)
5. *INFOSEC '93 Security Investigations* — 7/5/93

Commission of the European Communities, DGXIII/B
Roland Huber, Director DGXIII/B

6. *Information Security — INFOSEC '92 — Security Investigations* — 1/92
Senior Officials Group, Information Security (SOG-IS)

FEDERAL LAWS (U.S.)

1. Brooks Act (Pub. L. 89-306)
2. Paperwork Reduction Act (Pub. L. 96-511)
3. Warner (ASPA) Amendment (Pub. L. 97-86)
4. Federal Managers' Financial Integrity Act of 1982 (Pub. L. 97-225)
5. Paperwork Reauthorization Act of 1986 (Pub. L. 99-500)
6. Competition in Contracting Act (Pub. L. 98-369)
7. Computer Security Act of (Pub. L. 100-235)
8. Privacy Act of 1974 (Pub. L. 93-579)
9. Copyright Act of 1980 (17 USC)
10. Trade Secrets Act (18 USC 1905)
11. Patent and Trademark Laws (31 USC)
12. Electronic Communications Privacy Act (Pub. L. 99-508)
13. Counterfeit Access Device and Computer Fraud and Abuse Acts (Pub. L. 98-473, Pub. L. 99-474)
14. Public Printing and Documents Act (44 USC 33)
15. Computer Matching and Privacy Protection Act (Pub. L. 100-503)
16. Freedom of Information Act (Pub. L. 90-23)

FEDERAL REGULATIONS (U.S.)

1. Federal Acquisition Regulation (FAR) (48 CFR 1-51)
2. Federal Information Resources Management Regulation (FIRMR) (41 CFR 101)

INFOSEC BUSINESS ADVISORY GROUP (IBAG)

1. *INFOSEC Business Advisory Group, Draft Constitution, Rules of Procedure, Draft Objective*
Infosec Business Advisory Group (IBAG)
2. *The IBAG Framework for Commercial IT Security* — V 2.0, 9/93 (Replaces Discussion Draft, 2/93)
Infosec Business Advisory Group (IBAG)

COMMISSION OF THE EUROPEAN COMMUNITY (CEC)

1. *Proceedings of the Third Concertation Meeting for the Security Investigations Projects* — 6/18-19/92
Commission of the European Community (CEC)

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO)

1. *Internal Control — Integrated Framework* — 9/92
Committee of Sponsoring Organizations of the Treadway Commission (COSO)
Coopers & Lybrand, Author

COMMUNICATIONS SECURITY ESTABLISHMENT (CSE), GOVERNMENT OF CANADA

1. *Trusted Systems Environment Guideline* — (CID/09/17) Interim, 12/92
Communications Security Establishment (CSE), Government of Canada

DEPARTMENT OF DEFENSE (U.S.)

1. *Department of Defense Trusted Computer System Evaluation Criteria* — DOD 5200.28.STD (Orange Book), 12/85
Department of Defense Standard, U.S. Department of Defense

EDP AUDITORS FOUNDATION, INC.

1. *Control Objectives*, Copyright 1992
EDP Auditors Foundation, Inc.
David H. Li, Ph.D., CPA, Director of Research

GASSP COMMITTEE

1. *Generally Accepted Security Principles (GASP)*
   GASSP Committee
   Hal Tipton
2. *Generally Accepted System Security Principles* — Draft, Rev. 4.1., 3/30/94
   GASSP Committee
   Jim Appleyard

IBM

1. *Information Systems Security Controls and Procedures — Data Security Support Programs* — Third Edition, 2/86
   IBM

INFORMATION SYSTEMS SECURITY ASSOCIATION (ISSA)

1. *Information Systems Security Common Body of Knowledge* — 10/4/89
   ISSA Committee on the Information Systems Security Common Body of Knowledge
   Bill Murray, Chairman
2. *The Consensus Common Body of Knowledge* — 2nd Draft, 9/93
   The Forum Invitational Workshop on Information Technology Security Training and Professional Development
   Bill Murray, Chairman

INSTITUTE OF INTERNAL AUDITORS (IIA)

1. *Systems Auditability and Control (SAC)* — 1994
   Institute of Internal Auditors Research Foundation (IIA RF)

INTERNATIONAL STANDARDS ORGANIZATION (ISO)

1. *Resolutions Taken at the First Plenary Meeting of ISO/IEC JTC1/SC27, Stockholm, Sweden* — 4/24–26/90
   International Standards Organization (ISO) XC27 Secretariat

MINISTRY OF INTERNATIONAL TRADE AND INDUSTRY (MITI)

1. *Study Document for Assurance Requirements in Japanese Computer Security Criteria* — 10/93
   Ministry of International Trade and Industry (MITI)

NATIONAL FIRE PROTECTION ASSOCIATION

1. *The NFPA Standards-Making System*
   National Fire Protection Association
   Arthur E. Cote, P.E., Secretary, Standards Council

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (U.S.)

1. *Workshop on Security Procedures for the Interchance of Electronic Documents: Selected Papers and Results* — NISTIR 5247, 8/93
   National Institute of Standards and Technology (NIST)
   Roy G. Saltman, Editor
2. *Minimum Security Functionality Requirements for Multi-User Operating Systems* — Draft, Issue 1, 1/27/92, Federal Criteria Project #1
   National Institute of Standards and Technology (NIST), Computer Security Division
3. *Minimum Security Requirements for Multi-User Operating Systems* — A Protection Profile for the USA Information Security Standard, Issue 2, Federal Criteria Project #2, 8/7/92
   National Institute of Standards and Technology (NIST), Gaithersburg, MD
4. *Federal Criteria for Information Technology Security* — Volume I, Protection Profile Development — Version 1.0, Federal Criteria Project #3, 12/92
   National Institute of Standards and Technology (NIST) and National Security Agency (NSA)
5. *Federal Criteria for Information Technology Security Workshop Proceedings*

— Issue 1.0, Federal Criteria Project #4, 7/30/93
U.S. Department of Commerce, National Institute of Standards and Technology, Department of Defense, National Security Agency

OFFICE OF MANAGEMENT AND BUDGET (OMB) CIRCULARS (U.S.)

1. *OMB Circular A-123, Internal Control Systems*
2. *OMB Circular A-127, Financial Management Systems*
3. *OMB Circular A-130, Management of Federal Information Resources*

OFFICE OF PERSONNEL MANAGEMENT REGULATIONS (U.S.)

1. *The Office of Personnel Management's (OPM) Regulation (5 CFR 930)*
2. *OPM's Federal Personnel Manual (Ch. 731, 732, and 736)*

SYSTEM SECURITY STUDY COMMITTEE, NATIONAL RESEARCH COUNCIL (U.S.)

1. *Computers At Risk — Safe Computing in the Information Age* — 4/92
   System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD)

1. *Guidelines for the Security of Information Systems* — 11/26/92
   Organization for Economic Cooperation and Development (OECD)DG(92)190
2. *Ad Hoc Group of Experts on Guidelines for the Security of Information Systems* — 9/18/92
   Organization for Economic Cooperation and Development (OECD), Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy
3. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* — 9/23/81
   Organization for Economic Cooperation and Development (OECD)

PANACEA LIMITED, U.K.

1. *Information Systems Security and the Multinational Enterprise* — 11/8/93
   Panacea Limited, U.K.
   Clive W. Blatchford

SENSORMATIC ELECTRONICS CORPORATION

1. *Investment in the Future* — Computer and Information Security Embedded in Integrated Corporate Security Plan, Version 1.0, 6/93
   Sensormatic Electronics Corporation (Prepared for American Society for Industrial Security, ASIS)
   Samuel G. Shirley

SRI INTERNATIONAL

1. *I-4 Baseline Controls: A Checklist* — Draft, 4/93
   SRI International, International Information Integrity Institute (I-4)
2. *The Baseline Controls* — Copyright 1988
   SRI International, International Information Integrity Institute (I-4)
3. *Commercial International Security Requirements (CISR)* — 4/92
   SRI International, International Information Integrity Institute (I-4)
   Ken Cutler, American Express and Fred Jones, Electronic Data Systems

SIMPLOT DECISION CENTER, IDAHO STATE UNIVERSITY

1. *The Body of Knowledge* — Draft, 11/4/93
   Simplot Decision Center, Idaho State University
   Bill Murray, Chairman

Appendix D: GASSP Management Infrastructure

1. Framework

The GASSP infrastructure is in the process of being defined though a deliberative process of the GASSP Committee under the auspices of the International Information Security Foundation (I²SF) with input from other interested parties.

1.1 GASSP Governing Board

It is the committed purpose of the I²SF to sustain continued leadership and support this important effort. This effort was initiated as an ISSA President's Committee. The structure for the I²SF Committee for Generally Accepted System Security Principles (GASSP) is as follows.

1.1.1 GASSP Oversight Committee. The GASSP Oversight Committee, hereafter referred to as Oversight Committee, has been established to provide independent review of GASSP Committee operations, to coordinate liaison activities, to monitor the management process, and to perform quality assurance reviews. The Chair of the Oversight Committee is the I²SF Chairman of the Board of Directors. The Chair is to be initially assisted by a select committee of four (4) information systems security specialists: one representative from a standard-setting organization; one I²SF member who is a certified auditor; and two I²SF members who are Certified Information Systems Security Professionals. Members of the Oversight Committee may not be currently serving on the GASSP Committee. The Oversight Committee Chair will appoint the members of the Oversight Committee, with the concurrence of the I²SF Chairman. The Oversight Committee will periodically review the status and progress of the GASSP project and report the results to the I²SF Board of Directors.

1.1.2 GASSP Advisory Council. The Oversight Committee Chair, with input from the GASSP Committee Chair, will appoint, with the concurrence of the I²SF Chairman, an eight (8)-member GASSP Advisory Council, hereafter referred to as the Advisory Council. The Advisory Council will comprise four recognized information security specialists knowledgeable of the GASSP process, but not a member of the GASSP Committee, and will include a representative from the National Institute of Standards and Technology (NIST) and three representatives from the international community. One of the Advisory Council members will be appointed as the Advisory Council Chair by the Oversight Committee Chair. The Advisory Council will be responsible for reviewing and commenting on all GASSP Committee activities, products, and materials. The Advisory Council will provide its advice, and on a periodic schedule and upon request, written reports to the I²SF Board of Directors through the Oversight Committee Chair.

1.1.3 GASSP Committee. The GASSP Committee will select a chairperson. Working groups will be formed, drawing on GASSP Committee membership, to

address specific tasks in execution of the GASSP project plan (as represented in the GASSP Strategic and Business Plans). Tasks not specifically addressed by the plan, or requiring more specific guidance than provided by the plan, will require the development of a not-to-exceed one page description of each new task. The one-page task description will include a task summary (e.g., what is to be accomplished, how it will be completed), objectives, deliverables, milestones, and schedule for completion. The new task descriptions will be developed with the advice and consultation of the Advisory Council and be forwarded to the Oversight Committee Chair to provide advance notice of the work effort. The Oversight Committee Chair may provide guidance on new tasks as necessary. The GASSP Committee Chair will coordinate all GASSP activities with the Advisory Council and the Oversight Committee, which includes producing quarterly status reports of progress based on the GASSP plan, new tasks, and schedules. All GASSP products will be developed with the active advice and consultation of the Advisory Council in advance of being submitted to the Oversight Committee Chair. All communications of the GASSP Committee will be issued by either the I²SF Board of Directors or the GASSP Committee Chair following prior approval of the Oversight Committee Chair. All final products of the GASSP Committee will be issued or published by the Oversight Committee.

1.2 Information Security Principles Board

The GASSP Information Security Principles Board will consist of respected information security practitioners, industrialists, educators, and government employees. The board will:

☐ Publish proposed and approved opinions of the profession about accepted principles, standards, conventions, and mechanisms.
☐ Establish a process for gathering and evaluating comments about proposed opinions and including merited opinions in the GASSP.
☐ Establish processes for reporting and recommending disciplinary action to certified bodies for professional conduct not in accordance with GASSP.
☐ Establish processes for professionals to secure authorization to deviate from GASSP without censure or loss of certification.
☐ Utilize and support the Body of Knowledge upon which certification of information security professionals is based.

1.3 Information Security Profiles Board

An Information Security Profiles Board will be established to publish proposed and approved opinions regarding principles, standards, conventions, mechanisms to be included or adhered to in information technology products, and information security considerations. A product certification process and periodic audits of product compliance with GASSP will support these opinions. Product certification will be addressed by the Common Criteria.

The Common Criteria is a document and process being developed by NIST, NSA, and international organizations to create protection profiles that may be used by vendors to build information technology products that meet organizations' needs. The process of creating a profile includes a step for specifying evaluation criteria.