CORPORATE INFORMATION SECURITY WORKING GROUP

REPORT OF THE BEST PRACTICES AND METRICS TEAMS

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

GOVERNMENT REFORM COMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES

NOVEMBER 17, 2004

(Revised January 10, 2005)

TABLE OF CONTENTS

I. BACKGROUND

During Phase I of the Corporate Information Security Working Group (CISWG) convened in November 2003 by Representative Adam Putnam (R-FL), the Best Practices team surveyed available information security guidance. It concluded in its March 2004 report[1] that much of this guidance is expressed at a relatively high level of abstraction and is therefore not immediately useful as actionable guidance without significant and often costly elaboration. A one-page listing of Information Security Program Elements regarded as essential content for comprehensive enterprise management of information security was created, upon which it was hoped future actionable guidance could be built for use by a wide variety of organizations.

The Best Practices and Metrics teams of CISWG Phase II, convened in June 2004, were charged with expanding on the work of Phase I by refining the Information Security Program Elements and developing recommended Metrics supporting each of the elements. The goal was to develop a resource that would help Board members, managers, and technical staff establish their own comprehensive structure of principles, policies, processes, controls, and performance metrics to support the people, process, and technology aspects of information security.

This document represents the work of the members of the CISWG Phase II Best Practices and Metrics Teams whose contributions are gratefully acknowledged. Appendix E lists the team members who participated in development of this document.

It is important to provide appropriate attribution regarding two very helpful resources that were used as the starting point for developing the metrics described in this document:

(1) National Institute of Standards and Technology Special Publication 800-55, Security Metrics Guide for IT Systems (http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf), and

(2) The ISG Assessment Tool contained in the April 2004 Information Security Governance (ISG) Task Force report (http://www.cyberpartnership.org/InfoSecGov4_04.pdf). The lineage of the ISG Task Force Assessment Tool can be traced to the Corporate Information Security Evaluation for CEO's developed by TechNet (http://www.technet.org/).

The foundational work by NIST and the members of the CyberPartnership is acknowledged and appreciated. It gave the CISWG teams a substantial foundation upon which to develop numerically measurable metrics to aid information security management at the enterprise level.

---

[1] http://reform.house.gov/TIPRC/

II. INTRODUCTION

It is imperative that public and private sector organizations protect the information entrusted to them by various stakeholders against unauthorized access, disclosure, use, loss, or damage. Not only is this a basic fiduciary responsibility, but a growing body of external requirements mandates attention to information security. U.S. federal government agencies must demonstrate compliance with the Federal Information Security Management Act of 2002 (FISMA). Private sector organizations are subject to the information security implications of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act of 1999 (GLB), and the Sarbanes-Oxley Act of 2002 (SOX).

The ultimate responsibility for information security resides with the Board of Directors/Trustees in its role as keeper of the governance framework. Protecting information involves implementing information security principles, policies, processes and controls, and generally includes establishing performance standards and compliance metrics to support the framework and monitor whether or not information security is being effectively managed. The National Association of Corporate Directors has published helpful guidance related to Board oversight of information security[2].

The term "information" as used here includes information in human, physical, and electronic forms. Some information is often critical to the organization's success, such as that relating to products, processes, finance, customers, and copyrighted or patented intellectual property. Loss or compromise of certain information can be harmful or even fatal to an organization in terms of damage to its reputation, financial status, or its operational ability to function.

Basic fiduciary responsibilities include protection of shareholder interests, compliance with external requirements, and oversight of internal and external audits, all of which have information security implications. A balanced Information Security Program embraces a carefully selected set of foundational principles such as the guidelines promulgated by the Organization for Economic Cooperation and Development[3]. The Board should adopt a set of basic principles upon which it and management can build a structure of security policies, processes, controls, and performance metrics.

Effective management of information security typically involves reaching into all areas of the enterprise with special attention to critical assets and operational functions. Consequently, close collaboration among Board members, managers, and technical staff is essential. Generally, the first step is to identify and list information assets, properly classified with respect to confidentiality, integrity, availability, and privacy considerations. The same should be done for operational functions that are dependent upon information security.

Organizations should conduct a risk assessment – considering vulnerabilities, probabilities, and impact – to enumerate the unacceptable risks to which the information assets and functions are exposed, with priority emphasis placed on key corporate assets and functions. After understanding the risks, strategies, policies, and controls can be developed and implemented to eliminate, mitigate, or share those risks. Recognizing that total risk elimination is impossible, it is important for the Board to work with management to establish tolerable thresholds for identified risks for each identified information asset or information-dependent function. This enables the Board to convey its level of tolerance for the acceptance of various risks to executive management in a meaningful and measurable way. Organizations that have no

---

[2] "Information Security Oversight: Essential Board Practices" (2001), and "The Report of the NACD Blue Ribbon Commission on Risk Oversight" (2002). National Association of Corporate Directors.

[3] http://www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html

demonstrable need, based on a reasonable risk assessment, to implement a particular control do not need to implement that control and can still achieve best practices. However, those organizations that do have a demonstrable need for appropriate controls following such a reasonable risk assessment should consider the following controls and their suitability to their particular environment.

Equally important is for the Board to ensure that senior management makes clear assignments of key information security management roles, responsibilities, and accountabilities. The Board should ensure that appropriate enabling resources are provided. It should review information security policy and make information security a frequent board meeting agenda item. It may choose to assign information security to a board committee to ensure adequate oversight of and support for key information security leaders in the organization.

Executive management should make clear assignments of information security roles and responsibilities throughout the organization. Care should be taken to ensure that people assigned information security responsibilities possess the skills and certifications or experience appropriate for their assignment. Some information security and risk management knowledge is highly specialized and technical, some is managerial, and some involves general information security awareness and skills appropriate for everyone in the organization. Ideally, all employee job descriptions should include a clear definition of information security and privacy responsibilities and knowledge requirements. A record should be kept of employees' written acknowledgement of their responsibilities for privacy, protection of information, and acceptable use policies.

A popular dictum states, "What gets measured gets done." When a Board of Directors requires the CEO to report regularly the values of specified metrics, it communicates to the CEO what the directors consider important. Similarly, when a CEO requires managers to regularly report values of certain metrics, those managers know what is important to the CEO. It is up to the Board, management, and technical staff – working in close collaboration – to identify, approve, and articulate the set of metrics supporting the Information Security Program. In the technology realm, it is important that security products, technical configurations, and controls enable and effectively support policies established by management. For example, how long should a workstation with a logged-on user account be left inactive (and possibly unattended) before being automatically logged off? Many technical controls automate management policies such as this.

Metrics are about transforming policy into action and measuring performance. Visible metric scores provide a positive influence on human behavior by invoking the desire to succeed and compare favorably with one's peers. Metrics report how well policies, processes, and controls are functioning, and whether or not desired performance outcomes are being achieved. It should be noted that many of the metrics described herein measure the status or effectiveness of controls, not the underlying risks the controls are intended to mitigate. Risk measurement involves complex consideration of threat event frequency, probability of attack, exposure from vulnerabilities (mitigated in part by controls), and magnitude of potential loss.

Metrics also enable Continuous Improvement and Capability Maturity Models by providing a numerically objective way of scoring the status of a particular information security item on a continuous scale -- as distinguished from ranking an item according to a finite series of incremental steps toward maturity, e.g., (1) a policy has been documented for this item, (2) procedures supporting this policy have been documented, (3) the policy and procedures have been tested and reviewed, and (4) the policy and its supporting procedures have been fully integrated into the comprehensive information security program.

A process-oriented metric (e.g., percentage of employees who have satisfactorily completed information security training) will measure how fully the training **process** has been implemented, not necessarily its effectiveness. A metric measuring the **outcome** of a policy and its supporting procedures (e.g., percentage of security incidents that caused damage, compromise, or loss beyond established risk

thresholds) will generally reflect the maturity and effectiveness of the underlying policies, processes, and controls established to produce the desired outcome, in this case, as close to zero incidents as economically reasonable.

The Information Security Program Elements and Supporting Metrics described below are intended to help those in authority ensure appropriate steps have been taken to protect the organization's critical information assets plus the information supporting its key operational functions.

Although they are intended to be generic, these Information Security Program Elements and Supporting Metrics are not offered on a "one size fits all" basis. They are intended for voluntary internal use by boards, management, and technical staff, enabling them to monitor over time the status and progress of their information security program. Each organization should thoughtfully consider which Information Security Program Elements and Supporting Metrics might be helpful in its own circumstances. It should set its own implementation priorities and establish its own unique policy, process, and control structure with the level of detail it deems appropriate. Larger and more complex organizations will likely create policies, processes, and controls in each Program Element that are more extensive than those a smaller organization might choose to implement. To assist smaller enterprises, Appendix C recommends practices and metrics appropriate for Small and Medium Organizations (SMEs), defined by the U.S. Department of Commerce as organizations with fewer than 500 employees.

The suggested metrics, thresholds, and acceptable ranges are all subject to local definition, modification, and supplementation as desired. Terms such as "key," "critical," and "significant" are intentionally left to each organization to define in a manner meaningful to it. Some of the metric definitions can be inverted if desired, to drive toward a desired target value that is lower (zero-defects) rather than higher (100% compliance). Target values for metrics should be established by each organization in relation to its own circumstances and objectives. For many of the metrics, a value of 100% or 0% is impractical or unattainable, often because the consequence of accepting some risk is less than the cost of achieving perfection. The objective is to strive for the best value attainable after considering both the cost of the effort and the benefit of the result. It is up to each organization to decide whether or how it wants to manage the security of the information entrusted to it by its stakeholders.

Establishing an effective information security program producing desired results cannot be accomplished overnight. Rather, a determined long range perspective is appropriate, starting with a minimum baseline set of program elements and maturing the program over time. Appendix B lists those practices and metrics which constitute a minimum baseline program that organizations can use as a starting point after which they can work toward a more fully developed information management capability.

From a legal perspective, the information gathered and documented through the use of the suggested metrics may be considered sensitive. Further, there is a cost involved in implementing these recommendations in terms of executive and employee time, supporting technology, and financial resources. As with any approach chosen to manage risk, each organization will want to conduct its own cost- benefit analysis and determine the applicability of the guidance contained in this document to its internal information security program and the business environment being supported. During litigation, the discoverability of certain information could expose documented security weaknesses and result in legal liability in the United States. Compliance with privacy laws and other personal information regulations in the European Union and elsewhere also may impose limitations on the collection of data and documentation of employee policy violations and may expose an organization to additional liabilities.

III. RECOMMENDATIONS

1. The best practices and supporting metrics described in this document are practical and operationally actionable guidance useful in a wide variety of public and private sector organizations of varying sizes and types. Organizations are encouraged to voluntarily use this guidance as a resource whether seeking to initiate a new information security program or enhance an existing program. The use of these information security practices and supporting metrics will enable enterprises everywhere to better protect themselves from financial, operational, or reputational damage or loss resulting from unauthorized access, disclosure or use of the information entrusted to them by their stakeholders.

2. Using the information security management practices and metrics described in this document as a starting point, public sector agencies and the various private industry sectors are urged to immediately engage in the process of evolving sector-specific metric definitions and target values for sector-wide implementation. The objective is to lay the groundwork for a future capability enabling enterprise-to-enterprise and agency-to-agency comparisons within each sector -- thus creating an ongoing positive motivating influence toward improved information security program effectiveness throughout each of the sectors.

To this end, the following immediate follow-up steps are recommended:

(a) recruit one or more critical infrastructure sector and public sector entities interested in piloting information security best practices and metrics methodology derived from the content of this report,

(b) assemble one or more groups of selected professionals with appropriate information security management expertise at the board, management, and technical levels representing the academic research and practitioner perspectives,

(c) subject the content of this document to a rigorous review, refinement, and customization for pilot testing by the designated sector(s),

(d) Seek proposals from appropriate academic research entities interested in providing coordination and management support for this activity.

3. In the event that safe harbor legislation is contemplated for private sector organizations that have implemented a specified definition of minimum information security management practice, the Fundamental Five practices and associated metrics described in Appendix C are recommended as a very basic minimum level of information security management practice.

IV. HOW TO READ THIS DOCUMENT

This document consists of a main body and five appendices. In addition to a master listing of Information Security Program Elements, the main body lists each Program Element along with one or more suggested metrics supporting that element.

Appendix A provides a comparative listing of the full set of metrics described in this document, plus the baseline subset described in Appendix B and the subset for use by Small and Medium Enterprises (SMEs) listed in Appendix C.

Appendix B will help organizations choose an initial minimum baseline set of metrics. The baseline metrics, which are correlated with thirteen minimum essential information security practices, are intended to serve as a starting point. Committing to these practices serves as a baseline from which an organization can proceed toward implementation of a more complete set of metrics as it matures its information security capability. Minimum baseline metrics are identified with a **(B)** notation before the metric description in the main body of this document

Appendix C presents the "Fundamental Five" basic information security management practices plus a list of metrics recommended for SMEs (Small and Medium Enterprises), defined by the U.S. Department of Commerce as having less than 500 employees. The "Fundamental Five" practices and SME Metrics, identified with an **(SME)** notation before the metric, should be considered a starting point for SMEs, after which a more mature information security program can be developed over time.

Appendix D is a listing of references that can be helpful for an organization when writing its information security policies.

Appendix E acknowledges the individuals who contributed to the preparation of this document.

V. INFORMATION SECURITY PROGRAM ELEMENTS

A. GOVERNANCE (BOARD OF DIRECTORS/TRUSTEES)

1. Oversee Risk Management and Compliance Programs Pertaining to Information Security (e.g., Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley) (ISPE1)

2. Approve and Adopt Broad Information Security Program Principles and Approve Assignment of Key Managers Responsible for Information Security (ISPE2)

3. Strive to Protect the Interests of all Stakeholders Dependent on Information Security (ISPE3)

4. Review Information Security Policies Regarding Strategic Partners and Other Third-parties (ISPE4)

5. Strive to Ensure Business Continuity (ISPE5)

6. Review Provisions for Internal and External Audits of the Information Security Program (ISPE6)

7. Collaborate with Management to Specify the Information Security Metrics to be Reported to the Board (ISPE7)

B. MANAGEMENT

8. Establish Information Security Management Policies and Controls and Monitor Compliance (ISPE8)

9. Assign Information Security Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges (ISPE9)

10. Assess Information Risks, Establish Risk Thresholds and Actively Manage Risk Mitigation (ISPE10)

11. Ensure Implementation of Information Security Requirements for Strategic Partners and Other Third-parties (ISPE11)

12. Identify and Classify Information Assets (ISPE12)

13. Implement and Test Business Continuity Plans (ISPE13)

14. Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance (ISPE14)

15. Protect the Physical Environment (ISPE15)

16. Ensure Internal and External Audits of the Information Security Program with Timely Follow-up (ISPE16)

17. Collaborate with Security Staff to Specify the Information Security Metrics to be Reported to Management (ISPE17)

C. TECHNICAL

18. User Identification and Authentication (ISPE18)

19. User Account Management (ISPE19)

20. User Privileges (ISPE20)

21. Configuration Management (ISPE21)

22. Event and Activity Logging and Monitoring (ISPE22)

23. Communications, Email, and Remote Access Security (ISPE23)

24. Malicious Code Protection, Including Viruses, Worms, and Trojans (ISPE24)

25. Software Change Management, including Patching (ISPE25)

26. Firewalls (ISPE26)

27. Data Encryption (ISPE27)

28. Backup and Recovery (ISPE28)

29. Incident and Vulnerability Detection and Response (ISPE29)

30. Collaborate with Management to Specify the Technical Metrics to be Reported to Management *(ISPE30)*

VI. INFORMATION SECURITY PROGRAM ELEMENTS AND SUPPORTING METRICS FOR BOARDS OF DIRECTORS/TRUSTEES

Establishing an effective Information Security Program requires that Board members devote attention to the following Program Elements and the associated metrics. These metrics involve several implicit assumptions about what the Board and executive management should do in designing and implementing an Information Security Program, the extent of which will be influenced by the size and complexity of the organization.

- First, explicitly identify information assets and functions that are critical to the success of the organization.

- Second, assess the risks to which this information is potentially exposed, with respect to confidentiality, integrity, availability, and privacy.

- Third, establish acceptable thresholds for those risks.

- Fourth, identify, implement information security strategies, policies, and controls involving people, process, and technology to mitigate known risks and maintain these risks at acceptable levels.

As appropriate, a Board may consider delegating some of these tasks to a key standing committee, (such as the Audit Committee) or forming a special committee tasked with information security oversight.

1. ***Oversee Risk Management and Compliance Programs Pertaining to Information Security (e.g., Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, etc.)***

2. ***Approve and Adopt Broad Information Security Program Principles and Approve Assignment of Key Managers Responsible for Information Security***

3. ***Strive to Protect the Interests of all Stakeholders Dependent on Information Security***

4. ***Review Information Security Policies Regarding Strategic Partners and Other Third-parties***

5. ***Strive to Ensure Business Continuity***

6. ***Review Provisions for Internal and External Audits of the Information Security Program***

7. ***Collaborate with Management to Specify the Information Security Metrics to be Reported to the Board***

Below is a list of metrics suggested for Board use in connection with its information security responsibilities. With only a few exceptions, the metrics in this document are expressed as a percentage where a higher value is desirable. The exceptions involve: (1) metrics that are better understood when they are expressed such that a lower percentage value is desirable, and (2) those that are expressed as a number rather than a percentage. For metrics that are an exception to the general rule, a bold, and underlined comment in the note accompanying the metric states that a lower value is desirable.

1. *Oversee Risk Management and Compliance Programs Pertaining to Information Security (e.g., Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, etc.)*

   1.1. **(B) Percentage of key information <u>assets</u> for which a comprehensive strategy has been implemented to mitigate information security risks as necessary and to maintain these risks within acceptable thresholds**

   1.2. **Percentage of key organizational <u>functions</u> for which a comprehensive strategy has been implemented to mitigate information security risks as necessary and to maintain these risks within acceptable thresholds**

   1.3. (B) Percentage of key external requirements for which the organization has been deemed by objective audit or other means to be in compliance

   > Note: Various external requirements have different levels of significance or materiality to the organization, so it is important to understand the relative level of risk or impact represented by each external requirement with which the organization is out of compliance.

2. *Approve and Adopt Broad Information Security Program Principles and Approve Assignment of Key Managers Responsible for Information Security*

   2.1. **Percentage of Information Security Program Principles for which approved policies and controls have been implemented by management**

   > Note: The Board will likely want this metric to be reported for selected components of the organization responsible for critical information assets, objectives, or functions

   2.2. **(B) (SME) Percentage of key information security management roles for which responsibilities, accountabilities, and authority are assigned and required skills identified**

   > Note: Capable management is a critical element of the Information Security Program. The Board should carefully define and assign key information security management roles, responsibilities, and accountabilities.
   >
   > It is crucial to ensure key information security managers and others in the organization possess the information security knowledge and skills appropriate for their assignment. Various organizations award certifications that can serve as an indicator of the information security knowledge and experience possessed by a particular person. Available certifications include: CISSP (ISC2SM); CISA (ISACA®), and CISM (ISACA®); and the GIAC (SANS) certifications for various technologies. There are many others.

3. *Strive to Protect the Interests of all Stakeholders Dependent on Information Security*

   3.1. **Percentage of board meetings and/or designated committee meetings for which information security is on the agenda**

   Note: The Board should consider including information security on the agenda for every Board meeting, or at every meeting of the committee, if any, assigned to oversee information security.

   3.2. **(B) Percentage of security incidents did not that cause damage, compromise, or loss beyond established thresholds to the organization's assets, functions, or stakeholders**

   3.3. **Estimated damage or loss in dollars resulting from all security incidents**

   Note: All organizations experience security incidents where unauthorized access to information is attempted or achieved. Tracking the number of incidents that cause damage, compromise, or loss in relation to established risk thresholds as a percentage of the total number of incidents is a useful indication of the ultimate effectiveness of the organization's Information Security Program as well as the overall magnitude of incident activity. Analysis of the types of damage incurred will help devise improved defenses. The term "security incident" is used throughout the remainder of this document to mean events that threaten and/or cause damage, compromise, or loss of the organization's assets and/or functions. **(A lower value is desirable)**

4. *Review Information Security Policies Regarding Strategic Partners and Other Third-parties*

   4.1. **(B) Percentage of strategic partner and other third-party relationships for which information security requirements have been implemented in the agreements with these parties**

   Note: For the security of its own information, an organization often depends on third parties (e.g., strategic partners, consulting, outsourcing, and other parties) to whom it gives access to its information assets, or to whom it allows electronic connection with its networks. To mitigate risks associated with these relationships, the organization should include information security requirements in the agreements it has with these parties, and require demonstration of compliance.

5. *Strive to Ensure Business Continuity*

   5.1. **(B) Percentage of organizational units with an established business continuity plan**

   Note: Business continuity includes crisis management, disaster recovery, and incident management. Business continuity plans should consider provisions for recovery from various types of loss, including financial (via use of reserves or insurance), functional, and reputational, among others. The term "business continuity plan" encompasses plans for all business functions and their supporting processes. An "established" business continuity plan will also include evidence of successful testing of the plan's key components.

6. *Review Provisions for Internal and External Audits of the Information Security Program*

   6.1. **(B) Percentage of required internal and external audits completed and reviewed by the Board**

Note: Internal and external audit review information should be broken out by business process/function so the risk to each part of the organization is clearly identified. Audit findings should be ranked in order of significance/materiality so the risk and impact they represent can be understood. Management's response to audit findings in the form of planned action and/or results should be properly documented.

6.2. (B) Percentage of audit findings that have been resolved

Note: This metric will give visibility to progress being made in implementing corrective actions related to audit findings. This metric is an example of the particular importance of providing the numerator and denominator for the percentage to illustrate the overall extent of audit findings.

7. Collaborate with Management to Specify the Information Security Metrics to be Reported to the Board

Note: A carefully chosen set of information security metrics for management reports of information security status to the board will clarify to management what the board members consider important and on which they wish to be kept informed. Board members can choose their information security metrics from those defined above and/or create others they consider appropriate for the organization. For large enterprises, it is assumed the metrics will be calculated by various units of the organization and aggregated at various levels up to the entire enterprise. Each metric is reported for the current and last n reporting periods so trends and changes are visible (such as $n=3$ if quarterly reports are generated, to provide an annual perspective). For percentage metrics, the numerator and denominator as well as the resulting percentage, should be reported. The Board should specify reporting frequency and target values for the chosen metrics.

VII. INFORMATION SECURITY PROGRAM ELEMENTS AND SUPPORTING METRICS FOR MANAGEMENT

The following will help managers implement the information security goals and policies established by the Board. Establishing an effective Information Security Program requires management to devote attention to the following program elements:

8. Establish Information Security Management Policies and Controls and Monitor Compliance

9. Assign Information Security Roles, Responsibilities, Required Skills, and Role-based Information Access Privileges

10. Assess Information Risks, Establish Risk Thresholds and Actively Manage Risk Mitigation

11. Ensure Implementation of Information Security Requirements for Strategic Partners and Other Third-parties

12. Identify and Classify Information Assets

13. Implement and Test Business Continuity Plans

14. Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance

15. Protect the Physical Environment

16. Ensure Internal and External Audits of the Information Security Program with Timely Follow-up

17. Collaborate with Security Staff to Specify the Information Security Metrics to be Reported to Management

Below is a list of metrics suggested for management use in connection with its information security responsibilities. With only a few exceptions, the metrics in this document are expressed as a percentage where a higher value is desirable. The exceptions involve: (1) metrics that are better understood when they are expressed such that a lower percentage value is desirable, and (2) those that are expressed as a number rather than a percentage. For metrics that are an exception to the general rule, a bold, and underlined comment in the note accompanying the metric states that a lower value is desirable.

8. *Establish Information Security Management Policies and Controls and Monitor Compliance*

   8.1. **(B) Percentage of Information Security Program Elements for which approved policies and controls are currently operational**

   > Note: As a minimum, the overall information security policy structure and content should include the topics represented by the Information Security Program Elements defined in this document. It is also important for management to establish specific policies for the Technical Information Security Program Elements on topics such as encryption, event and activity logging, user identification and authentication, configuration management, and others. Information security policies and controls should be managed and monitored by senior management, and approved by the board of directors/trustees.

   8.2. **(B) (SME) Percentage of staff assigned responsibilities for information security policies and controls who have acknowledged accountability for their responsibilities in connection with those policies and controls**

   8.3. **(B) Percentage of information security policy compliance reviews with no violations noted**

   8.4. **Percentage of business unit heads and senior managers who have implemented operational procedures to ensure compliance with approved information security policies and controls**

9. *Assign Information Security Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges*

   > Note: This element defines and assigns all information security roles and responsibilities and describes the skills necessary to fulfill these roles. In addition, this element reviews and enforces role-based access privileges assigned to each information asset or class of asset as identified in ISPE12.

   9.1. **(B) (SME) Percentage of new employees hired this reporting period who satisfactorily completed security awareness training before being granted network access**

   9.2. **(B) (SME) Percentage of employees who have satisfactorily completed periodic security awareness refresher training as required by policy**

   9.3. **Percentage of position descriptions that define the information security roles, responsibilities, skills, and certifications for:**

      a. *Security Managers and Administrators*

      b. *IT personnel*

*c. **General staff system users***

9.4. **Percentage of job performance reviews that include evaluation of information security responsibilities and information security policy compliance**

9.5. **(B) (SME) Percentage of user roles, systems, and applications that comply with the separation of duties principle**

Note: This metric can be difficult to enforce and measure. However, separation of duties is a vital element of internal controls requiring close coordination between information security and the owners/operators of business application systems. It is incumbent upon security management to ensure coordinated separation of duties controls across the full spectrum of system, processing, and functional activities. Auditors should be expected to routinely assess the effectiveness of separation of duties controls in their assessment of compliance with laws, regulations, and policies.

9.6. **(B) Percentage of individuals with access to security software who are trained and authorized security administrators**

9.7. **(B) Percentage of individuals who are able to assign security privileges for systems and applications who are trained and authorized security administrators**

9.8. **Percentage of individuals whose access privileges have been reviewed this reporting period**

*a. **(B) (SME) Employees with high level system and application privileges***

*b. **(B) (SME) Terminated employees***

9.9. **Percentage of users who have undergone background checks**

Note: Consider users with high-level system privileges as well as those who have access to information assets deemed critical via risk assessment.

10. ***Assess Information Risks, Establish Risk Thresholds and Actively Manage Risk Mitigation***

10.1. **(B) (SME) Percentage of critical information assets and information-dependent functions for which some form of risk assessment has been performed and documented as required by policy**

10.2. **Percentage of critical assets and functions for which the cost of compromise (loss, damage, disclosure, disruption in access to) has been quantified**

Note: Costs of compromise include violations of confidentiality, availability, integrity, and privacy considerations, plus direct costs of loss or damaged data or systems, loss of future income or sales, costs of potential litigation (defense costs, settlements and judgments), costs of potential regulatory actions, lost opportunity costs and impact on reputation such as market capitalization. Methods for quantifying these costs in some sectors are more advanced in some sectors, such as financial services, than others. Each organization should determine methods appropriate for its circumstances.

10.3. **(B) (SME) Percentage of identified risks that have a defined risk mitigation plan against which status is reported in accordance with policy**

11. *Ensure Implementation of Information Security Requirements for Strategic Partners and Other Third-parties*

Note: For the security of its own information, an organization often depends on third parties (e.g., strategic partners, consulting, outsourcing, and other parties) to whom it gives access to its information assets, or to whom it allows electronic connection with its networks. To mitigate risks associated with these relationships, it should include information security requirements in the agreements it has with these parties, and require demonstration of compliance.

11.1. **Percentage of known information security risks that are related to third-party relationships**

Note: **A lower value is desirable.**

11.2. **(B) (SME) Percentage of critical information assets or functions for which access by third-party personnel is not allowed**

11.3. **(B) (SME) Percentage of third-party personnel with current information access privileges who have been reviewed by designated authority to have continued need for access in accordance with policy**

11.4. **(B) (SME) Percentage of systems with critical information assets or functions for which electronic connection by third-party systems is not allowed**

11.5. **Percentage of security incidents that involved third-party personnel**

Note: **A lower value is desirable.**

11.6. **Percentage of third-party agreements that include/demonstrate external verification of policies and procedures**

11.7. **(B) (SME) Percentage of third-party relationships that have been reviewed for compliance with information security requirements**

11.8. **Percentage of out-of-compliance review findings that have been corrected since the last review**

12. *Identify and Classify Information Assets*

12.1. **(B) (SME) Percentage of information assets that have been reviewed and classified by the designated owner in accordance with the classification scheme established by policy**

Note: Not all information assets can be protected at the highest level. Protection priorities, decisions, and corresponding investments should be based on an assessment of risk to the asset, the asset's value, the impact if the asset is compromised (lost, damaged, disclosed, access disrupted), and consideration of the cost to reconstitute the asset vs. the cost to protect the asset.

12.2. **Percentage of information assets with defined access privileges that have been assigned based on role and in accordance with policy**

Note: The identification and classification of any information asset should include access privileges to that asset (create, read, write, edit/modify, delete, etc.). Such privileges should be assigned to specific roles within the organization as identified in ISPE9.

12.3. **Percentage of scheduled asset inventories that occurred on time according to policy**

Note: This metric assumes the existence of asset inventories that are regularly updated based on events (such as the addition or retirement of critical information assets) or periodically such as quarterly.

13. *Implement and Test Business Continuity Plans*

Note: Business continuity includes crisis management, disaster recovery, and incident management. The term "business continuity plan" encompasses plans for all of these functions and their supporting processes. Incident Management includes prevention, preparation, detection, response, recovery/restoration, and improvement. The Incident Management Plan includes vulnerability assessment and management of at least systems on which critical information assets reside and that support critical information-dependent functions.

13.1. **(B) Percentage of organizational units with a documented business continuity plan for which specific responsibilities have been assigned**

Note: This plan should address information, hardware/facility, process/capability, and human elements of business continuity, and take third-party relationships into account. As well, it should include provision for recovery of various types of loss, including financial, operational, and reputational.

13.2. **(B) Percentage of business continuity plans that have been reviewed, exercised/tested, and updated in accordance with policy**

14. *Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance*

Note: This element applies to review and approval of the information systems architecture for compliance with information security requirements and policies, and for any impacts to information security during the architecture's life cycle.

14.1. **Percentage of information security risks related to systems architecture identified in the most recent risk assessment that have been adequately mitigated.**

14.2. **(B) Percentage of system architecture changes (additions, modifications, or deletions) that were reviewed for security impacts, approved by appropriate authority, and documented via change request forms**

14.3. **Percentage of critical information assets or functions residing on systems that are currently in compliance with the approved systems architecture**

15. *Protect the Physical Environment*

15.1. **(B) (SME) Percentage of critical organizational information assets and functions that have been reviewed from the perspective of physical risks such as controlling physical access and physical protection of backup media**

15.2. **Percentage of critical organizational information assets and functions exposed to physical risks for which risk mitigation actions have been implemented**

15.3. **(B) (SME) Percentage of critical assets that have been reviewed from the perspective of environmental risks such as temperature, fire, flooding, etc.**

15.4. **Percentage of servers in locations with controlled physical access**

16. *Ensure Regular Internal and External Audits of the Information Security Program with Timely Follow-up*

    16.1. **(B) Percentage of information security requirements from applicable laws and regulations that are included in the internal/external audit program and schedule**

    16.2. **(B) Percentage of information security audits conducted in compliance with the approved internal/external audit program and schedule**

    16.3. **(B) Percentage of management actions in response to audit findings / recommendations that were implemented as agreed as to timeliness and completeness**

17. *Collaborate with Security Staff to Specify the Information Security Metrics to be Reported to Management*

Note: A carefully chosen set of information security metrics for reports to management of information security status will clarify to operational units what management considers important and the topics on which management wishes to be informed. Management can choose its set of information security metrics from those defined above and/or create others considered appropriate for the organization. For large enterprises, it is assumed the metrics will be calculated by various units of the organization and aggregated at various levels up to the entire enterprise. Each metric is reported for the current and last *n* reporting periods so trends and changes are visible (such as *n*=3 if quarterly reports are generated, to provide an annual perspective). For percentage metrics, the numerator and denominator as well as the resulting percentage, should be reported. Management should specify reporting frequency and target values for the chosen metrics.

VIII. INFORMATION SECURITY PROGRAM ELEMENTS AND SUPPORTING METRICS – TECHNICAL

Technical controls are those controls contained within and executed by the various information technology environments such as Microsoft Windows®, Sun Solaris™, Linux, Cisco IOS®, etc. For each of the Technical Program Elements, multiple technical controls are commonly available within each of the various technologies.

Many, if not most, of an organization's information security policies will ultimately be implemented by assigning values to technical security controls within the various information technology environments. For example, it is common to set a technical control for automatically logging off active user sessions on idle workstations after a certain number of minutes. The policy value for a technical control such as this is generally established by adopting a recognized standard such as the Center for Internet Security consensus benchmarks[4], and then making local adaptations as appropriate. The ability to automate technical controls that implement and demonstrate compliance with certain information security policies represents a powerful security resource that a security-conscious organization can use to its benefit.

Establishing a complete Information Security Program requires attention to the following technical program elements:

18. User Identification and Authentication

19. User Account Management

20. User Privileges

21. Configuration Management

22. Event and Activity Logging and Monitoring

23. Communications, Email, and Remote Access Security

24. Malicious Code Protection

25 .Software Change Management, including Patching

26. Firewalls

27. Data Encryption

28. Backup and Recovery

29. Incident and Vulnerability Detection and Response

30. Collaborate with Management to Specify the Technical Metrics to be Reported to Management

The metrics defined herein represent a minimum baseline and are therefore not exhaustive. The technical program element metrics chosen by a particular organization are influenced by the perceived risks and associated information security principles and policies adopted and promulgated by its governing board

---

[4] http://www.cisecurity.org

and management. The controls of value to various organizations will vary according to size and complexity, the specific risks being mitigated, the efficacy attributed to certain controls, and available technical security expertise.

18. *User Identification and Authentication*

   18.1. **(B) (SME) Number of active user IDs assigned to only one person**

   18.2. **(B) (SME) Percentage of systems and applications that perform password policy verification**

   18.3. **(B) (SME) Percentage of active user passwords that are set to expire in accordance with policy**

   18.4. **Percentage of systems with critical information assets that use stronger authentication than IDs and passwords in accordance with policy**

   Note: A user name and password is called "single-factor authentication" or "weak authentication." Strong authentication requires using at least two of a possible three factors: something you know (a user ID, password, or PIN), something you have (a security device you plug into a USB port), and something you are (a retina scan or fingerprint). Therefore, an example of strong authentication would be a password (something you know: factor #1 and a fingerprint (something you are: factor #2).

   A risk-based approach to authentication developed by the financial sector is described in the following references:

   http://www.occ.treas.gov/ftp/advisory/2001-8a.pdf

   http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

19. *User Account Management*

   19.1. **(B) (SME) Percentage of systems where vendor-supplied accounts and passwords have been disabled or reset**

   Note: Systems often come with vendor-supplied accounts such as guest accounts and vendor-supplied passwords for administrator accounts. In general, vendor-supplied accounts should be disabled and vendor-supplied passwords should be changed, since they are generally widely known.

   19.2. **(B) (SME) Percentage of computer user accounts assigned to personnel who have left the organization or no longer have need for access that have been closed**

   Note: Computer accounts include user accounts as well as system, group, application, or superuser accounts.

   19.3. **(B) Percentage of systems with account lockout parameters set in accordance with policy**

   19.4. **Percentage of inactive user accounts that have been disabled in accordance with policy**

19.5. **(B) (SME) Percentage of workstations with session time-out/automatic logout controls set in accordance with policy**

Note: Analysis of illegal insider activity has shown that leaving a workstation unattended that is logged into a user account is an invitation to inappropriate access by persons other than the one to whom the user account is assigned. Automatic log-off and password-protected screensavers are examples of how an automated technical control can be used to enforce organizational policy (in this case, session control policy) on a real-time basis.

20. *User Privileges*

20.1. **(B) (SME) Percentage of active computer accounts that have been reviewed for justification of current access privileges in accordance with policy**

Note: Computer accounts include user accounts as well as system, group, application, or superuser accounts.

20.2. **(B) (SME) Percentage of systems where permission to install non-standard software is limited in accordance with policy**

Note: Unauthorized installation of non-approved software is one way malicious software (viruses, Trojans, and worms) finds it way onto an organization's systems. Accordingly, a policy of discipline based on the following security principles is considered baseline security practice. First, users should not have administrative access or control over organization-owned systems. Second, the only software authorized for procurement is that which is included in the organization's approved software suite. Third, only persons authorized by management are allowed to install that software on the organization's systems. Fourth, exceptions to the above policies based on a valid business case can be authorized on a case basis by designated management.

20.3. **Percentage of systems and applications where assignment of user privileges is in compliance with the policy that specifies role-based information access privileges**

21. *Configuration Management*

21.1. **Percentage of systems for which approved configuration settings have been implemented as required by policy**

21.2. **(B) (SME) Percentage of systems with configurations that do not deviate from approved standards**

Note: Management should establish specific approved system configurations as policy for each operating system environment. The approved configurations will generally be based on a recognized standard of practice and some degree of local deviation that may be justified by operational necessity. The number of deviations from approved configurations should be kept to a minimum via a waiver process. An important configuration control is to disable unneeded services and to only allow them to be enabled in the course of a managed change process.

21.3. **(B) (SME) Percentage of systems that are continuously monitored for configuration policy compliance with out-of-compliance alarms or reports**

21.4. **Percentage of systems whose configuration is compared with a previously established trusted baseline in accordance with policy**

Note: One of the most effective ways to ensure malicious code has not been inadvertently installed on a running system is to periodically compare its entire 'footprint' or configuration with a previously established trusted baseline that is stored in a secure location. This comparison can reveal the presence of unexpected files or changes to files that can then be analyzed further. The trusted baseline is updated when the configuration incorporates authorized changes.

21.5. **(B) Percentage of systems where the authority to make configuration changes is limited in accordance with policy**

22. *Event and Activity Logging and Monitoring*

22.1. **(B) Percentage of systems for which event and activity logging has been implemented in accordance with policy**

22.2. **(B) (SME) Percentage of systems for which event and activity logs are monitored and reviewed in accordance with policy**

22.3. **Percentage of systems for which log size and retention duration have been implemented in accordance with policy**

22.4. **(B) Percentage of systems that generate warnings about anomalous or potentially unauthorized activity**

23. *Communications, Email, and Remote Access Security*

23.1. **(B) (SME) Percentage of notebooks and mobile devices that are required to verify compliance with approved configuration policy prior to being granted network access**

Note: When they connect to the enterprise network, notebooks and other mobile devices not properly configured and protected with anti-virus, personal firewall, intrusion detection and integrity checking software can introduce malicious software (viruses, worms, and Trojan horses) into the network. Before being granted network access, such devices should be automatically checked by a software utility to ensure they are using the security protections required by policy.

23.2. **Percentage of communications channels controlled by the organization that have been secured in accordance with policy**

Note: When sensitive information is sent by file transfer, Web pages (HTML), or instant messaging over the Internet and other unprotected links, it is possible for someone other than the intended receiver to see the information. Web servers should have certificates for authentication, and sensitive information on Web pages should be protected with SSL/TLS and authentication of client users. Virtual private networks that use IPSEC or web-based SSL/TLS will secure communications involving transactions, file transfers, etc. Alternatively, a general encryption utility can be used to encrypt a sensitive file before sending the file using instant messaging, or FTP. Security policy should describe what information requires protection when sent over an open network such as the Internet and the appropriate security mechanism to be used. Unless the organization is prepared to encrypt all data traffic across the network

regardless of sensitivity, email encryption falls outside the scope of this control. However, users should be educated about email encryption, and email encryption for sensitive information is both highly recommended and encouraged.

23.3. Percentage of host servers that are protected from becoming relay hosts

Note: Spammers look for unprotected email servers they can use to forward spam mail. They also look for other servers where they can install mail relay software to relay their spam mail. In addition to using your network resources, the spam coming from your Internet address can damage your reputation and result in other organizations blocking all mail from your address. Email servers should restrict relaying from external sources.

23.4. Percentage of mobile users who access enterprise facilities using secure communications methods

Note: Remote users who use unprotected access when connecting to an organizational network, risk disclosing user ID and passwords as well as sensitive company information. When users access the organization over an open network they should use a secure connection such as a virtual private network (VPN) using SSL/TLS or IPSEC or a secure web based session (SSL/TLS). Wireless users should use WEP or preferably WPA to protect against disclosure. IEEE 802.1x should be considered for authenticating both wireless and wired remote users.

24. *Malicious Code Protection, Including Viruses, Worms, and Trojans*

24.1. (B) (SME) Percentage of workstations (including notebooks) with automatic protection in accordance with policy

24.2. (B) (SME) Percentage of servers with automatic protection in accordance with policy

24.3. (B) (SME) Percentage of mobile devices with automatic protection in accordance with policy

25. *Software Change Management, including Patching*

25.1. (B) (SME) Percentage of systems with the latest approved patches installed

Note: If this metric is not reported as 100%, rationale should be provided as to why particular patches have not been installed. It is advisable to test and approve patches in a non-production environment before operational deployment to identify possible adverse impact on functionality or interoperability of operational software. An organization may make a conscious decision to delay patch deployment or eliminate a patch from deployment consideration. This should be done only after careful consideration of the criticality of the system(s) involved plus the vulnerabilities and risks involved in not deploying the patch.

25.2. Mean time from vendor patch availability to patch installation by type of technology environment

Note: **A lower value is desirable.**

25.3. **(B) Percentage of software changes that were reviewed for security impacts in advance of installation**

26. *Firewalls*

   26.1. **(B) (SME) Percentage of workstation firewalls, host firewalls, sub-network firewalls, and perimeter firewalls configured in accordance with policy**

27. *Data Encryption*

   27.1. **(B) Percentage of critical information assets stored on network accessible devices that are encrypted with widely tested and published cryptographic algorithms**

   27.2. **(B) (SME) Percentage of mobile computing devices using encryption for critical information assets in accordance with policy**

   27.3. **Percentage of passwords and PINS that are encrypted (cryptographically one-way hashed) in accordance with policy**

28. *Backup and Recovery*

   28.1. **(B) (SME) Percentage of systems with critical information assets or functions that have been backed up in accordance with policy**

   28.2. **(B) (SME) Percentage of systems with critical information assets or functions where restoration from a stored backup has been successfully demonstrated**

   28.3. **(B) (SME) Percentage of backup media stored offsite in secure storage**

   28.4. **Percentage of used backup media sanitized prior to reuse or disposal**

29. *Incident and Vulnerability Detection and Response*

   29.1. **(B) Percentage of operational time that critical services were unavailable (as seen by users and customers) due to security incidents**

   Note: Operational time excludes scheduled maintenance and downtime. This metric assumes critical services have been identified as part of a risk assessment. **A lower value is desirable.**

   29.2. **(B) (SME) Percentage of security incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds**

   Note: **A lower value is desirable.**

   29.3. **Percentage of systems affected by security incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds**

   Note: **A lower value is desirable.**

   29.4. **(B) Percentage of security incidents that were managed in accordance with established policies, procedures, and processes**

   Note: The intent is to measure the percentage of successful attacks that were handled in accordance with policy, defined procedures, and in-place processes in a disciplined,

repeatable, predictable manner. Such behavior assumes the existence of well-defined processes for incident management. This is contrasted with responding to an attack in an ad-hoc, chaotic manner. "Managed" includes detecting an incident, containing an incident and its effects, analyzing the damage caused by an incident and preventing its recurrence, taking corrective action, and restoring services and systems in a timely manner.

29.5. **(B) (SME) Percentage of systems with critical information assets or functions that have been assessed for vulnerabilities in accordance with policy**

29.6. **(B) (SME) Percentage of vulnerability assessment findings that have been addressed since the last reporting period**

30. *Collaborate with Management to Specify the Technical Metrics to be Reported to Management*

Note: For large enterprises, the metrics can be calculated by various units of the organization and aggregated at various levels up to the entire enterprise. Each metric is reported for the current and last *n* reporting periods so trends and changes are visible (such as *n*=3 if quarterly reports are generated, to provide an annual perspective). For percentage metrics, the numerator and denominator as well as the resulting percentage, should be reported. Reporting frequency and target values for the technical metrics should be specified by management as part of its Information Security Program policies.

APPENDIX A – COMPARATIVE METRICS SUMMARY

1. The full set of metrics listed in this document

Implementation of the full set of metrics described in this document would involve an undertaking unlikely to be practical even in large enterprises. The full set is intended to serve as a reference set from which to begin as deemed appropriate within a particular organization at the board, management, and technical levels. In all organizations, including relatively large and sophisticated ones, implementation of information security metrics is best accomplished over a period of time, beginning with a subset of the full set described in this document. Implementation of additional metrics can then occur over time as the organization's information security management capability matures.

2. Baseline Metrics

To assist with the selection of an initial set with which to begin, Appendix B lists a baseline subset of metrics correlated with a minimum essential list of information security management practices.

3. Metrics for Small and Medium Enterprises (SMEs)

Small and medium enterprises (defined by the U.S. Department of Commerce as those having less than 500 employees) are unlikely to have the resources and sophistication available to larger organizations. Consequently, a more modest subset of metrics, correlated with basic practices appropriate for SMEs, is listed in Appendix C.

4. A comparative summary of All, Baseline, and SME metrics

The following table will be helpful in comparing the baseline and SME subsets with the full set of metrics described in this document.

Summary of All, Baseline, and SME Metrics		
All Metrics	**Baseline**	**SME**
Board		
1.1	X	
1.2		
1.3	X	
2.1		
2.2	X	X
3.1		
3.2	X	
3.3		
4.1	X	
5.1	X	
6.1	X	
6.2	X	
Subtotal 12	8	1

Summary of All, Baseline, and SME Metrics		
All Metrics	**Baseline**	**SME**
Management		
8.1	X	
8.2	X	X
8.3	X	
8.4		
9.1	X	X
9.2	X	X
9.3a		
9.3b		
9.3c		
9.4		
9.5	X	X
9.6	X	
9.7	X	
9.8a	X	X
9.8b	X	X
9.9		
10.1	X	X
10.2		
10.3	X	X
11.1		
11.2	X	X
11.3	X	X
11.4	X	X
11.5		
11.6		
11.7	X	X
11.8		
12.1	X	X
12.2		
12.3		
13.1	X	
13.2	X	
14.1		
14.2	X	
14.3		
15.1	X	X
15.2		
15.3	X	X
15.4		
16.1	X	
16.2	X	
16.3	X	
Subtotal	42	25	15

Technical			
	18.1	X	X
	18.2	X	X
	18.3	X	X
	18.4		
	19.1	X	X
	19.2	X	X
	19.3	X	
	19.4		
	19.5	X	X
	20.1	X	X
	20.2	X	X
	20.3		
	21.1		
	21.2	X	X
	21.3	X	X
	21.4		
	21.5	X	
	22.1	X	
	22.2	X	X
	22.3		
	22.4	X	
	23.1	X	X
	23.2		
	23.3		
	23.4		
	24.1	X	X
	24.2	X	X
	24.3	X	X
	25.1	X	X
	25.2		
	25.3	X	
	26.1	X	X
	27.1	X	
	27.2	X	X
	27.3		
	28.1	X	X
	28.2	X	X
	28.3	X	X
	28.4		
	29.1	X	
	29.2	X	X
	29.3		
	29.4	X	
	29.5	X	X
	29.6	X	X
Subtotal	45	32	24
Grand Total	99	65	40

APPENDIX B – BASELINE INFORMATION SECURITY PRACTICES AND METRICS

1. Introduction

The purpose of this Appendix is to highlight a suggested set of baseline information security metrics, identified with a (**B**) notation in the listing of metrics in this document. The selection of baseline metrics derives from thirteen minimum essential information security practices described below.

Minimum essential practices (and metrics that demonstrate them) **are intended to serve as a starting point** in an organization's journey toward effective information security. Committing to these practices serves as a logical first step toward implementing additional metrics from the complete set of metrics listed in this document.

The definition of minimum essential includes those practices deemed necessary for basic security hygiene and responsible citizenship, particularly when an organization's networks are connected to and accessible via the Internet or other third parties.

Baseline metrics are intended to demonstrate the presence of a practice as well as verification that the practice is operational (such as via compliance reviews and audits). In addition to the (**B**) notation in the main section of this document, each of the baseline metrics for governance (**G**), management (**M**), and technical (**T**) are mapped to each practice below.

2. Minimum Essential Practices with Companion Metrics

KEY: **G** = Governing Body (Board of Directors/Trustees), **M** = Management, **T** = Technical

1. The organization has implemented various levels of electronic and physical protection for its information assets (information, systems, networks, applications) including critical assets requiring the greatest level of protection and oversight. Protection actions are based on some form of risk assessment.

G 1.1

M 10.1, 10.3, 12.1, 15.1, 15.3

T 27.1, 27.2

2. A configuration management process is operational. All workstations, servers, laptops, routers, firewalls, and other network devices are built using a minimum essential configuration benchmark. This includes disabling all services that are not required, eliminating vendor supplied defaults for passwords, accounts, and security parameters, and continuous monitoring of system and device configuration status.

T 19.1, 19.3, 19.5, 21.2, 21.3, 23.1

3. A change management process is operational for all IT hardware and software. Changes are managed, deployed, and can be rolled back in accordance with a defined process. Security patches are subject to this process.

M 14.2

T 25.1, 25.3

4. Anti-virus software is installed on all systems. Signature updates and scans are performed automatically (daily).

T 24.1, 24.2, 24.3

5. Firewalls are used as an architectural component to (at least) separate public servers from internal organizational networks. Firewalls may also be used to separate internal sub-networks where access restriction is important.

T 26.1

6. All users are required to attend security awareness training prior to being granted access to the organization's networks and periodically as condition of continued access.

M 9.1, 9.2

7. Basic identity management mechanisms (authentication, authorization, access control) for access to both physical and electronic assets are implemented and regularly reviewed. This includes in-house access, remote access, and third party access.

M 9.6, 9.7, 9.8 (a, b), 11.2, 11.3

T 18.1, 18.2, 18.3, 19.1, 19.2, 20.1, 21.5

8. All information security management, technical, and user roles and responsibilities are explicitly assigned and assignments acknowledged.

G 2.2

M 8.2, 9.5

9. A business continuity plan is implemented and regularly tested. All critical assets are routinely backed up. Ability to selectively restore from backups is tested regularly.

G 5.1

M 13.1, 13.2

T 28.1, 28.2, 28.3

10. Information security policies are in force for acceptable use, incident response/reporting, and each of the baseline areas included in this document. Management visibly supports and enforces these policies. All users understand the consequences of non-compliance.

M 8.1, 8.3

T 20.2 (acceptable use)

11. Regular monitoring and review is conducted for:

- alert mechanisms, system logs for critical systems, firewall logs, incident reports, configuration violations
- vulnerability assessment results
- the overall security program

G 3.2

T 22.1, 22.2, 22.4, 29.1, 29.2, 29.4, 29.5, 29.6

12. The practices noted above are required in all third party service level agreements for those parties having access to organizational networks.

G 4.1

M 11.2, 11.3, 11.4, 11.7

13. Compliance with external (legal, regulatory) requirements is regularly demonstrated via internal and external audit. Audit findings are resolved in a timely manner.

G 1.3, 6.1, 6.2

M 16.1, 16.2, 16.3

APPENDIX C – INFORMATION SECURITY PRACTICES AND METRICS FOR SMALL AND MEDUIM ENTERPRISES

1. Introduction

The purpose of this Appendix is to suggest a set of information security metrics for small and medium-sized enterprises[5], identified with a (**SME**) notation in the listing of metrics in this document. The selection of SME metrics derives from thirteen minimum essential information security practices described in Appendix B, twelve of which are applicable to SMEs. The first five of these twelve are called the "Fundamental Five" and serve as a recommended initial starting point if the enterprise is unable to initially commit to all SME metrics.

Minimum essential practices (and the metrics that demonstrate them) **are intended to serve as a starting point** in an organization's journey toward effective information security. Committing to the "Fundamental Five" or all minimum essential practices and their companion SME metrics serves as a logical first step toward implementing additional metrics from the baseline list in Appendix B as well as the complete set of metrics listed in main body of this document.

The definition of minimum essential includes those practices deemed necessary for basic security hygiene and responsible citizenship, particularly when an organization's networks are connected to and accessible via the Internet or other third parties.

SME metrics are intended to demonstrate the presence of a practice along with some level of monitoring and review. In addition to the "SME" notation in the main section of this document, each of the SME metrics for governance (**G**), management (**M**), and technical (**T**) are mapped to each practice below. The "Fundamental Five" practices and their supporting metrics are listed first, followed by the remaining minimum essential practices for which SME metrics are recommended.

---

[5] Defined by the U.S. Department of Commerce as having fewer than 500 employees.

2. Minimum Essential ("Fundamental Five") Practices

The "Fundamental Five" practices are:

1. Malware protection, including worms and viruses

2. Change management, including patch management

3. Identity and access management, including privilege assignment and authentication

4. Firewalls including workstation, host, sub-network, and perimeter as required

5. Configuration management

3. Companion SME Metrics

KEY: **G** = Governing Body (Board of Directors/Trustees), **M** = Management, **T** = Technical

1. Anti-virus software is installed on all systems. Signature updates and scans are performed automatically (daily).

T 24.1, 24.2, 24.3

2. A change management process is operational for all IT hardware and software. Changes are managed, deployed, and can be rolled back in accordance with a defined process. Security patches are subject to this process.

T 25.1

3. Basic identity management mechanisms (authentication, authorization, access control) for access to both physical and electronic assets are implemented and regularly reviewed. This includes in-house access, remote access, and third party access and controls necessary to ensure identity and privacy protection.

M 9.8 (a, b), 11.2, 11.3

T 18.1, 18.2, 18.3, 19.1, 19.2, 20.1

4. Firewalls are used as an architectural component to (at least) separate public servers from internal organizational networks. Firewalls may also be used to separate internal sub-networks where access restriction is important.

T 26.1

5. A configuration management process is operational. All workstations, servers, laptops, routers, firewalls, and other network devices are built using a minimum essential configuration benchmark. This includes disabling all services that are not required, eliminating vendor supplied defaults for passwords, accounts, and security parameters, and continuous monitoring of system and device configuration status.

T 19.1, 19.5, 21.2, 21.3, 23.1

6. The organization has implemented various levels of electronic and physical protection for its information assets (information, systems, networks, applications) including critical assets requiring the greatest level of protection and oversight. Protection actions are based on some form of risk assessment.

M 10.1, 10.3, 12.1, 15.1, 15.3

T 27.2

7. All users are required to attend security awareness training prior to being granted access to the organization's networks and periodically as condition of continued access.

M 9.1, 9.2

8. All information security management, technical, and user roles and responsibilities are explicitly assigned and assignments acknowledged.

G 2.2

M 8.2, 9.5

9. In taking the first step towards a business continuity plan, all critical assets are routinely backed up. Ability to selectively restore from backups is tested regularly.

T 28.1, 28.2, 28.3

10. Information security policies are in force for acceptable use, incident response/reporting, and each of the SME practices included in this Appendix. Management visibly supports and enforces these policies. All users understand the consequences of non-compliance.

T 20.2 (acceptable use)

11. Regular monitoring and review is conducted for:

- alert mechanisms, system logs for critical systems, firewall logs, incident reports, configuration violations
- vulnerability assessment results
- the overall security program

T 22.2, 29.2, 29.5, 29.6

12. The practices noted above are required in all third party service level agreements for those parties having access to organizational networks.

M 11.2, 11.3, 11.4, 11.7

APPENDIX D – SOURCES FOR DEVELOPING INFORMATION SECURITY POLICIES

1. Definition of Terms

POLICY, STANDARD, OR GUIDELINE[6]

Frequently the terms "policy," "standard," and "guideline" are used to refer to documents that fall within the policy infrastructure. For clarity of terminology, a policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities. A standard is typically a collection of system-specific or procedural-specific requirements that must be met by everyone. For example, there might be a standard that describes how to harden a Windows NT® workstation for placement on an external (DMZ) network. People must follow this standard exactly if they wish to install a Windows NT® workstation on an external network segment. A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.

Primer for Developing Security Policies

For an introduction to setting Information Security Policy, see Michele D. Guel's "A Short Primer for Developing Security Policies."[7]

2. References to Information Security Policy

FREE RESOURCES AVAILABLE ON THE WEB

- ISSA (Information Systems Security Association-ISSA®): http://www.issa.org/gaisp/gaisp.html (free access) "Generally Accepted Information Security Principles."

- SANS (SysAdmin, Audit, Network, Security): http://www.sans.org/resources/policies/ (free access) Model policies.

- http://www.sans.org/rr/catindex.php?cat_id=50 (free access) Policy issue discussion white papers.

- http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf (free access) While paper on writing effective and enforceable security policies.

- http://secinf.net/ipolicye.html (free access) A large catalog of documents arranged topically. Cross references to SANS and other sites listed here.

- CISCO (Cisco®): http://www.cisco.com/warp/public/126/secpol.html (free access). Discusses Acceptable Use Policy.

---

[6] From the SANS Policy Project at http://www.sans.org/resources/policies/.

[7] Available at http://www.sans.org/resources/policies/Policy_Primer.pdf.

▪ JANET: http://www.ja.net/documents/JANET_security_policy.html (free access). Discusses Acceptable Use Policy.

▪ http://www.yourwindow.to/information-security/ (free access). An on-line glossary of information security terms.

▪ OSU (Ohio State University): http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc2196.html (free access) IETF RFC 2196 - Site Security Handbook.

▪ http://www.fcc.gov/hspc/ (free access) National Strategies to Secure Cyberspace and for the Protection of Critical Infrastructure and Key Assets

▪ http://www.ietf.org/html.charters/ipsp-charter.html (free access) IETF RFC 3586 IP Security Policy Requirements

▪ http://www.jisc.ac.uk/index.cfm?name=pub_smbp_infosec (free access) Guidance on Developing a Security Policy

▪ http://nces.ed.gov/help/privacy.asp (free access) National Center for Educational Statistics (NCES) - Web Privacy and Security Policy

▪ UCB (University of California-Berkeley): http://ist-socrates.berkeley.edu:2002/IT.sec.policy.html (free access) Berkeley Security Policies

▪ http://www.wustl.edu/policies/infosecurity.html (free access) Washington University at St. Louis Security Policies

▪ SD (SecurityDocs™): http://www.securitydocs.com/Security_Policies/Sample_Policies (free access) Catalog of Policies.

▪ http://www.occ.treas.gov/ftp/advisory/2001-8a.pdf

▪ http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf A risk-based approach to authentication developed by the financial sector is described in the above references.

COMMERCIAL/FEE BASED RESOURCES

(Disclaimer: This listing is just a beginning list of resources to assist in policy development. This should not be construed as an endorsement of any of the resources listed, nor intention to slight any of the good resources not listed).

▪ http://www.information-security-policies-and-standards.com/ SOS/RUsecure Information Security Policies - available on-line in MS Word and Adobe pdf format, $595.00

▪ http://www.network-and-it-security-policies.com/ IT/Network and Information Security Policies Download, available as a download / extract - resulting in Adobe pdf, MS Word and RTF format documents, $595.00

▪ http://www.security.kirion.net/securitypolicy/ COBRA Policy Compliance Analyst, price not disclosed.

▪ http://www.infoedge.com/product_detail.asp?sku1=1086111& Best Practice IT Security Policies Generator, ISO Security Solutions, 9/2004, $399.00 26 Sample Policies and Worksheets in Word format plus a 325-page supporting education package delivered with a supporting software package written using Microsoft Access® 2002. This set of "Best Practice" IT Security Policies has been written and developed for organizations of all size. Using this IT Security Policy Generator (requires Microsoft Access® 2002) in conjunction with the Policy Worksheets and Sample Policies provided allows you to immediately create customized IT Security Policies. Here in one place is everything you need to

develop, implement and manage 26 essential IT security policies that are based on the most-widely used international standards.

- Wood, Charles Cresson, Information Security Policies Made Easy Version 9, Baseline Software; (September 30, 2002), 727 pages, hardcover, ISBN: 1881585093, $795.00

- Wood, Charles Cresson, Information Security Roles & Responsibilities Made Easy, Version 1, Baseline Software; (May 1, 2001), 242 pages, hardcover, ISBN: 1881585085, $495.00

- Barman, Scott, Writing Information Security Policies, Sams; 1st edition (November 9, 2001), 214 pages, ISBN: 157870264X, $34.99

- Peltier, Thomas R., Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management, CRC Press; 1st edition (December 20, 2001), 312 pages, paperback, ISBN: 0849311373, $56.66

INFORMATION SECURITY PROGRAM ELEMENTS (ISPE) REFERENCING POLICY AND REFERENCES TO MODEL POLICIES

ISPE2. Approve and Adopt Broad Information Security Program Principles and Approve Assignment of Key Managers Responsible for Information Security

Metric Reference - 2.1

- SANS - Ethics Policy
- SANS - Acceptable Use Policy
- CISCO - Acceptable Use Policy
- JANET - Acceptable Use Policy
- UCB - Acceptable Computer Use Policy
- SD - Acceptable Use Policy

ISPE9. Assign Information Security Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges

Metric Reference - 9.3

- UBC - Roles and Responsibilities

ISPE10. Assess Information Risks, Establish Risk Thresholds and Actively Manage Risk Mitigation

Metric Reference - 10.1, 10.3

- SANS - Risk Assessment Policy

ISPE11. Ensure Implementation of Information Security Requirements for Strategic Partners and Other Third-parties

Metric References - 11.2, 11.7

- SANS - Third Party Network Connection Agreement Policy
- SANS - Application Service Provider Policy
- SANS - Extranet Policy
- SD - Extranet Policy

ISPE12. Identify and Classify Information Assets

Metric Reference - 12.1

- SANS - Information Sensitivity Policy

ISPE14. Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance

Metric Reference - 14.2

- SANS - Acquisition Policy
- SANS - Server Security Policy
- SD - Patching Policy

ISPE18. User Identification and Authentication

Metric References - 18.2, 18.3, 18.4

- SANS - Database Credentials Coding Policy
- SANS - Password Protection Policy
- OSU - Authentication
- SD - Password Policy

ISPE20. User Privileges

Metric References - 20.1, 20.2, 20.3

- OSU - Authorization
- OSU - Confidentiality
- OSU - Access
- UCB - Privileged Access Agreement Policy

ISPE22. Event and Activity Logging and Monitoring

Metric References - 22.1, 22.2, 22.3

- OSU - Auditing

ISPE23. Communications, Email, and Remote Access Security

Metric References - 23.1, 23.2, 23.3, 23.4

- SANS - Remote Access Policy
- SANS - Email Retention Policy
- SANS - Email Policy
- SANS - Dial In Access Policy
- SANS - Forwarded Email Policy
- SANS - Line Policy

- SANS - Router Policy
- SANS - VPS Security Policy
- SANS - Wireless Policy
- SD - Email Policy
- SD - Remote Access Policy
- SD - Wireless Policy

ISPE24. Malicious Code Protection, Including Viruses, Worms, and Trojans

Metric References - 24.1, 24.2, 24.3

- SANS - Anti-Virus Policy
- SD - Anti-Virus Policy

ISPE26. Firewalls

Metric References - 26.1

- SANS - DMZ Lab Security
- OSU - Firewalls

ISPE27. Data Encryption

Metric References - 27.1, 27.2, 27.3

- SANS - Encryption Policy

ISPE28. Backup and Recovery

Metric References - 28.1

- OSU - Securing Backups

ISPE29. Incident and Vulnerability Detection and Response

Metric References - 29.4, 29.5

- SANS - Vulnerability Scanning Policy
- OSU - Security Incident Handling

APPENDIX E – BEST PRACTICES AND METRICS TEAMS MEMBERS

The following CISWG Phase II Team members participated in the development of this document. Their contributions are gratefully acknowledged.

INFORMATION SECURITY BEST PRACTICES AND GUIDING PRINCIPLES TEAM

- Clint Kreitner – Center for Internet Security - Coordinator
- Michael Dickson – AICPA - Coordinator
- John Carlson – The Financial Services Roundtable/BITS
- Robert Daniels – ISSA
- Emily Frye – Critical Infrastructure Protection Project
- Leslie Saul Garvin – TechNet
- Brett Kilbourne – United Telecom Council
- Jim Kohlenberger/Dexter Ingram/Robert Tai – Business Software Alliance
- Rodney Petersen – EDUCAUSE
- Michael Rasmussen – Forrester Research
- Mark Silver – The Business Roundtable
- Karyn Waller – AICPA

ADJUNCT MEMBERS

- Julia Allen – Carnegie Mellon University/SEI
- Phil Campbell – Sandia Labs
- Chrisan Herrod – Securities & Exchange Commission
- Michael Hines – Purdue University
- Don Holden – Concordant, Inc.
- Alexandra Lajoux – National Association of Corporate Directors
- Charles Le Grand – The Institute of Internal Auditors, Inc.
- Adam Stone – Assurant, Inc.
- Jack Suess – University of Maryland, Baltimore County

PERFORMANCE METRICS, REPORTING, AND INFORMATION SHARING TEAM

- Charles Le Grand – The Institute of Internal Auditors - Coordinator
- Clint Kreitner – Center for Internet Security - Coordinator
- Cristin Flynn/Maggie Mansourkia – U. S. Internet Service Provider Association
- Paul Kurtz – Cyber Security Industry Alliance
- Jim Lewis – Center for Strategic & International Studies
- Alan Paller – The SANS Institute
- Michael Rasmussen – Forrester Research

ADJUNCT MEMBERS

- Julia Allen – Carnegie Mellon University/SEI
- Phil Campbell – Sandia Labs
- Dan Daly – Subcommittee staff
- Mike Dickson – AICPA
- Chrisan Herrod – Securities & Exchange Commission
- Michael Hines – Purdue University
- Don Holden – Concordant, Inc.
- Susan Kennedy – University of Pennsylvania
- Alexandra Lajoux – National Association of Corporate Directors
- Dan Swanson – The Institute of Internal Auditors
- Adam Stone – Assurant, Inc.
- Karyn Waller – AICPA