

Chief Security Officer

G U I D E L I N E

ASIS INTERNATIONAL COMMISSION ON GUIDELINES

The Commission on Guidelines was established in early 2001 by ASIS International (ASIS) in response to a concerted need for guidelines regarding security issues in the United States. As the preeminent organization for security professionals worldwide, ASIS has an important role to play in helping the private sector secure its business and critical infrastructure, whether from natural disaster, accidents, or planned actions, such as terrorist attacks, vandalism, etc. ASIS had previously chosen not to promulgate guidelines and standards, but world events have brought to the forefront the need for a professional security organization to spearhead an initiative to create security advisory provisions. By addressing specific concerns and issues inherent to the security industry, security guidelines will better serve the needs of security professionals by increasing the effectiveness and productivity of security practices and solutions, as well as enhancing the professionalism of the industry.

Mission Statement

To advance the practice of security through the development of risk mitigation guidelines within a voluntary, non-proprietary, and consensus-based process utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership and the security industry.

Goals and Objectives

- Assemble and categorize a database of existing security-related guidelines
- Develop methodology for identifying new guideline development projects
- Involve/organize ASIS Councils to support guideline development
- Identify and develop methodology for development, documentation, and acceptance of guidelines
- Develop and sustain alliances with related organizations to benchmark, participate, and support ASIS guideline development
- Produce national consensus-based guidelines in cooperation with other industries and the Security Industry Standards Council

Functions

- Establish guideline project
- Determine guidelines for development and assign scope
- Assign participating Council(s), where appropriate
- Approve membership on guideline committee
- Act as a governing body to manage and integrate guidelines from various Councils and security disciplines
- Review and monitor projects and guideline development
- Approve Final Draft Guideline and Final Guideline
- Select guidelines for submission to the Security Industry Standards Council and the American National Standards Institute (ANSI)



Chief Security Officer (CSO) Guideline

1.0	Title.....	3
2.0	Revision History.....	3
3.0	Commission Members.....	3
4.0	Committee Members	3
5.0	Acknowledgment	4
6.0	Guidelines Designation	4
7.0	Scope	4
8.0	Summary of Guideline.....	4
9.0	Purpose	4
10.0	Overview.....	4
11.0	Reporting Relationship	5
12.0	Model Function.....	5
	12.1 Model Profile Diagram	6
13.0	Key Responsibilities and Accountabilities.....	7
	13.1 Key Success Factors	7
	13.2 Strategy Development.....	7
	13.3 Information Gathering and Risk Assessment	8
	13.4 Organization Preparedness	8
	13.5 Incident Prevention	8
	13.6 Securing People, Core Business, Information, and Reputation.....	8
	13.7 Incident Response, Management, and Recovery	9
	13.8 Investor Relations, Public Affairs, and Government Relations Coordination	9
14.0	Key Competencies	9
15.0	Experience.....	11
16.0	Education	11
17.0	Compensation.....	11
	APPENDIX A	13

Copyright © 2004 by ASIS International

ISBN 1-887056-52-1

ASIS International (ASIS) disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance.

All rights reserved. Permission is hereby granted to individual users to download this document for their own personal use, with acknowledgment of ASIS International as the source. However, this document may not be downloaded for further copying or reproduction nor may it be sold, offered for sale, or otherwise used commercially.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

1.0 TITLE

The title of this document is the Chief Security Officer (CSO) Guideline.

2.0 REVISION HISTORY

Baseline Document

3.0 COMMISSION MEMBERS

Sean A. Ahrens, CPP, Schirmer Engineering
Norman D. Bates, Esq., Liability Consultants, Inc.
Regis W. Becker, CPP, PPG Industries
Jerry J. Brennan, Security Management Resources, Inc.
Chad Callaghan, CPP, Marriott International, Inc.
Pamela A. Collins, Ed.D., CFE, Eastern Kentucky University
Michael A. Crane, CPP, IPC International Corporation
Edward J. Flynn, CFE, Protiviti, Inc.
F. Mark Geraci, CPP, Bristol-Myers Squibb Co.
L. E. Mattice, Boston Scientific Corp.
Basil J. Steele, CPP, Sandia National Laboratories
Don W. Walker, CPP, Securitas Security Services USA, Inc.

4.0 COMMITTEE MEMBERS

Donald P. Bitner, Amgen
Keith D. Blakemore, CPP, Boise Office Solutions
Jerry J. Brennan, Security Management Resources, Inc.
David Burrill, British American Tobacco
George K. Campbell, Security Risk Management Consultancy
John C. Cholewa III, CPP, Sprint Corp.
Grant R. Crabtree, CPP, ALLTEL Corp.
Joseph A. DiDona, Reader's Digest Association, Inc.
Robert F. Fox, Sprint Corp.
Timothy L. Gladura, Cardinal Health, Inc.
John Hartmann, The Home Depot
Robert W. Hayes, CPP, CFE, Business Security Advisory Group, LLC
Michael A. Howard, Microsoft Corporation
Don L. Hubbard, PricewaterhouseCoopers LLP
Mark S. Lex, CPP, Abbott Laboratories
Robert F. Littlejohn, CPP, Avon Products Inc.
John E. McClurg, Lucent Technologies, Inc.
Raymond A. Mislock, Jr., E. I. duPont de Nemours & Co.
David R. Saenz, Levi Strauss & Co.
Victor E. Thuotte, Jr., Fidelity Investments
Reginald J. Williams, CPP, The Boeing Company
Timothy L. Williams, CPP, Nortel Networks
W. Lance Wright, USEC Inc.

5.0 ACKNOWLEDGMENT

ASIS International would like to express its foremost appreciation to W. Lance Wright, Vice President Human Resources & Administration, USEC Inc., author of the original Chief Security Officer (CSO) white paper presented at the 2002 ASIS Annual Seminar and Exhibits, for his time, assistance, and use of material, which contributed significantly to the development of this Guideline.

6.0 GUIDELINES DESIGNATION

This Guideline is designated as ASIS GDL CSO 06 2004.

7.0 SCOPE

The Chief Security Officer (CSO) Guideline has applicability in both the private and public sector environments, which must evaluate and respond to the continually increasing and changing risks to their assets and organizations both domestically and globally.

8.0 SUMMARY OF GUIDELINE

The CSO Guideline is designed as a tool to allow an organization to decide upon and provide a security architecture characterized by appropriate awareness, prevention, preparedness, and response to changes in threat conditions. This Guideline is structured at a high level, although specific considerations and responses also are addressed for consideration by individual organizations based on specific risk assessment and requirements.

9.0 PURPOSE

ASIS International has developed the CSO Guideline as a model for organizations to utilize in the development of a leadership function to provide a comprehensive, integrated security risk strategy to contribute to the viability and success of the organization.

10.0 OVERVIEW

Today's business risk environments have become increasingly more severe, complex, and interdependent, both domestically and globally. The effective management of these environments is a fundamental requirement of business. Boards of Directors, shareholders, key stakeholders, and the public correctly expect organizations to identify and anticipate areas of risk and set in place a cohesive strategy across all functions to mitigate or reduce those risks. In addition, there is an expectation that management will respond in a highly effective manner to those events and incidents that threaten the assets of the organization. A proactive strategy for mitigation of the risk of loss ultimately provides a positive impact to profitability and is an organizational governance responsibility of senior management and governing boards.

It is the thesis of this Guideline that the skills and competencies essential to active protection and measurably effective response to the modern threat environment are far more critical than ever before. Effective leadership within the top levels of the organization and its related security functions are imperative. Organizational reputation, the uninterrupted reliability of the technical