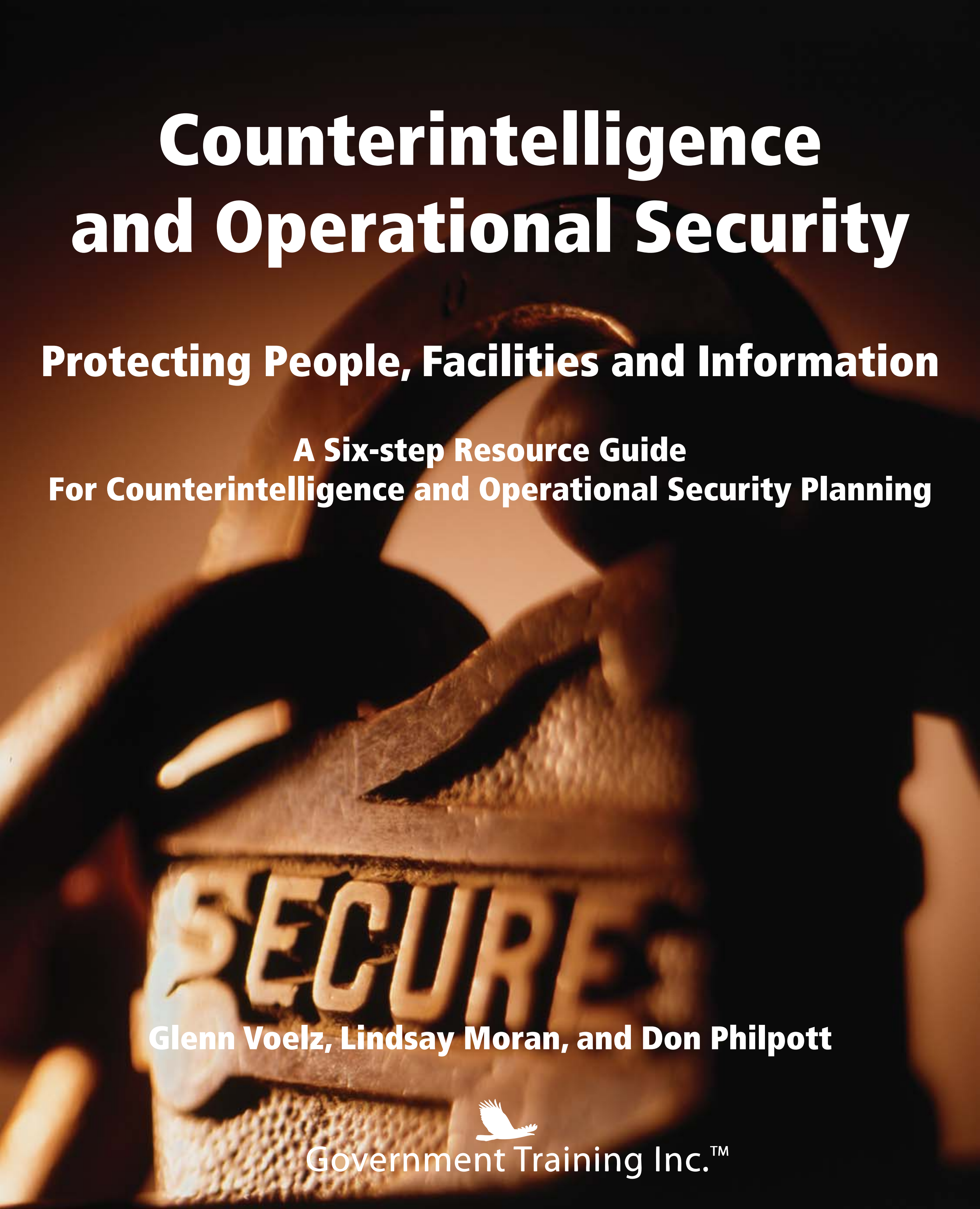

Counterintelligence and Operational Security

Protecting People, Facilities and Information

A Six-step Resource Guide For Counterintelligence and Operational Security Planning

Glenn Voelz, Lindsay Moran, and Don Philpott

Government Training Inc.™

About the Publisher – Government Training Inc.™

Government Training Inc. provides worldwide training, publishing and consulting to government agencies and contractors that support government in areas of business and financial management, acquisition and contracting, physical and cyber security and intelligence operations. Our management team and instructors are seasoned executives with demonstrated experience in areas of Federal, State, Local and DoD needs and mandates.

For more information on the company, its publications and professional training,
go to www.GovernmentTrainingInc.com.

Printed in the United States of America.

For information regarding permissions, write to:

Government Training Inc.

Rights and Contracts Department

5372 Sandhamn Place

Longboat Key, Florida 34228

don.dickson@GovernmentTrainingInc.com

ISBN: 978-1-937246-71-6

www.GovernmentTrainingInc.com

Sources:

This book has drawn heavily on the authoritative materials published by a wide range of sources.

These materials are in the public domain, but accreditation has been given both in the text and in the reference section if you need additional information.

The author and publisher have taken great care in the preparation of this handbook, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions.

No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or recommendations contained herein.

About the authors

Glenn Voelz

Glenn Voelz served in a variety of military and intelligence community assignments, including positions on the Joint Chiefs of Staff, in the Pentagon's National Military Command Center, and White House Situation Room. During his career, he commanded an Army counterintelligence and human intelligence company, served as Assistant Professor of History at West Point and as the senior intelligence advisor to the Saudi Arabian Ministry of Defense, among other military and intelligence community assignments. He is the author of several recent journal articles and books, including Managing the Private Spies: The Use of Commercial Augmentation for Intelligence Operations, and Contractors in the Government Workplace: Managing the Blended Workforce.

He holds a Bachelor of Science degree from the United States Military Academy at West Point, a Master of Arts from the University of Virginia, and a Master of Science in Strategic Intelligence from the National Defense Intelligence College.

Lindsay Moran

Lindsay Moran was an operations officer in the Central Intelligence Agency's clandestine service from 1998-2003. Her bestselling memoir "Blowing My Cover," vetted by the CIA prior to publication, went on to receive widespread critical acclaim. Ms. Moran's articles and opinions have appeared in The New York Times, The Washington Post, USA Today, Government Executive, Washingtonian and various other publications. She has served as a commentator on security and intelligence issues for CNN, ABC, MSNBC and Fox Networks, as well as other national and local radio outlets. From 2007-2009, Ms. Moran served as a Brand Representative for 3M Privacy Filters, making regular national media and corporate appearances to discuss Data and Personal Security in the USA and Canada.

Ms. Moran is a graduate of Harvard College (BA magna cum laude in English Literature, 1991; undergraduate commencement orator) and Columbia University (MFA in Writing, 1994). She was an English Literature teacher and a Fulbright Scholar prior to her service with the CIA.

Ms. Moran has lectured at Harvard University's John F. Kennedy School of Government, Yale College, the American Enterprise Institute, University of Virginia, American University, and various other colleges and universities. She also has spoken at numerous corporate conferences and literary festivals.

Currently, Ms. Moran works as a freelance writer and editor, consultant and speaker.

Don Philpott

Don Philpott is editor of International Homeland Security Journal and has been writing, reporting and broadcasting on international events, trouble spots and major news stories for almost 40 years. For 20 years he was a senior correspondent with Press Association-Reuters, the wire service, and traveled the world on assignments including Northern Ireland, Lebanon, Israel, South Africa and Asia.

He writes for magazines, and newspapers in the United States and Europe, and is a regular contributor to radio and television programs on security and other issues. He is the author of more than 100 books on a wide range of subjects and has had more than 5,000 articles printed in publications around the world. His most recent books are Handbooks for COTRs, Performance Based Contracting, Cost Reimbursable Contracting, How to Manage Teleworkers, Crisis Communications and Integrated Physical Security Handbook II. He is a member of the National Press Club.

Foreword

This handbook offers a comprehensive, up-to-date reference for organizational counterintelligence and operational security programs. It provides a logical introduction to the field of counterintelligence and operational security. Extensive citations and references facilitate additional study and research. The text introduces a six-step process for developing an organizational counterintelligence and operational security strategy. It also serves as a comprehensive resource of best practices, checklists, and tips for counterintelligence planners and security managers. Additionally, the handbook provides a practical tool for developing workforce counterintelligence and security awareness, as well as training and education programs to enhance the protection of people, facilities and information.

The handbook draws heavily on authoritative materials published by a wide range of government and private sector organizations including the Office of the National Counterintelligence Executive (ONCIX), the Federal Bureau of Investigation (FBI) the Department of Defense (DoD) and Department of Homeland Security (DHS), as well leading private sector organizations in the fields of counterintelligence, operational security and cyber defense. All materials referenced in this work reside in the public domain, and full accreditation is provided in Endnotes and the reference section of the handbook.

Acknowledgement

This handbook is based on research drawn from a wide variety of government regulations, manuals, training programs, academic journals, web resources, private sector studies and professional periodicals. Its contents are based entirely on widely accessible, open source materials residing in the public domain. No classified, sensitive or otherwise restricted materials were referenced, cited or consulted in the research and preparation of this handbook. Instances where excerpts, figures, quotes and secondary source materials directly appear in the text have been annotated with endnotes and appear as referenced sources in the Endnotes Section.

The views and opinions expressed in this handbook are the authors' own and do not reflect the official policy or position of the Department of Defense or U.S. Government. The manuscript was reviewed and approved for publication by the CIA Publications Review Board and Department of Defense Office of Security Review. Approval of these offices does not imply endorsement of the handbook or verification of its contents.

The authors and publisher have taken great care in the preparation of this handbook but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or recommendations contained herein.

Contents

Appendices for this publication are located at www.GovernmentTrainingInc.com.

Symbols

Throughout this book you will see a number of icons displayed. The icons are there to help you as you work through the Six Step process. Each icon acts as an advisory – for instance alerting you to things that you must always do or should never do. The icons used are:

❗ This is something that you must always do

⊘ This is something you should never do

💡 Really useful tips

⚑ Points to bear in mind

☑ Have you checked off or answered everything on this list?

Preface

Our adversaries – foreign intelligence services, terrorists, foreign criminal enterprises and cyber intruders – use overt, covert, and clandestine activities to exploit and undermine U.S. national security interests. Counterintelligence is one of several instruments of national power that can thwart such activities, but its effectiveness depends in many respects on coordination with other elements of government and with the private sector… the potential consequences of counterintelligence failures can be immediate and devastating, putting in jeopardy our nation's vital information, infrastructure, military forces, and a wide range of U.S. interests, technologies and personnel around the world.[1]

Economic, political and technological transformations of the past decade have significantly expanded the scope of intelligence threats faced by the U.S. government, business and industry. According to Michelle Van Cleave, former National Counterintelligence Executive, the "United States has become the single most important collection target in the world. Intelligence operations against the United States are now more diffuse, aggressive, technologically sophisticated and potentially more successful than ever before."[2] For this reason, FBI Director Robert Mueller recently designated espionage as the bureau's number two priority second only to terrorism on the FBI's list of threats to U.S. security and national interest.[3]

The end of the Cold War only complicated the challenge of defending against foreign intelligence threats. In the post-Cold-War era, the types of collectors and their targets have become more varied and difficult to identify. Foreign governments, private interests and terrorists alike employ a wide range of sophisticated technical surveillance tools in addition to traditional human intelligence tradecraft to access government, business and industrial information. National borders, traditional law enforcement and security methodologies no longer offer guaranteed deterrence against an adversary's intelligence collection efforts.

Remember

The expansion of multinational operations, digital information systems, wireless communication and web-based business practices all present new opportunities for exploitation by adaptive antagonists who need not step foot on U.S. soil to exploit security vulnerabilities and gather information. In short, our enemies have become savvier, hard to detect and even harder to deter.

Additionally, the scope of potential targets has expanded beyond those of traditional state-based espionage. Global economic competition has created a high premium for access to cutting-edge technology, trade secrets and proprietary information. The incentive for aggressive targeting of industrial information and military technology has never been higher as foreign companies seek a competitiveness edge in the worldwide marketplace. Furthermore, foreign intelligence services, economic competitors and international terrorist groups no longer distinguish between government and private industry. The latter owns and operates approximately 85 percent of the nation's critical infrastructures and key assets, including the defense industrial base, public health, energy, finance, transportation sectors, and the backbone of the nation's information and telecommunications networks.[4]

Estimate of the Problem

1. Over 100 countries are known to be actively involved in intelligence collection efforts against the United States.

2. China, Russia and India have been identified as top foreign collectors of U.S. technology and industrial secrets.[5]

3. Over the last two years, more than 40 Chinese and American citizens have been convicted of espionage-related charges.[6]

4. Intellectual property theft costs American corporations $250 billion a year.7 Theft of intellectual property and trade secrets costs 750,000 U.S. jobs a year.[8]

5. The estimated financial impact of individual cases of economic espionage range from less than $10,000 to more than $5.5 million per incident, totaling billions in losses to the U.S. economy each year.[9]

Foreign intelligence activities and private interests routinely target U.S. corporations and government agencies in order to gain access to business information, sensitive technology and proprietary trade secrets. For the government, sensitive information loss undermines national security, military advantage and relations with foreign nations. For American companies and industry it means loss of market share, potential profits, valuable intellectual property, trade secrets and reputation.

Vulnerability to such threats has only multiplied as government and the private sector increasingly collaborate with foreign partners and conduct business in a virtual workplace where the control of data and sensitive information is not always assured. These dynamics present ample opportunity for exploitation by foreign intelligence services, rival corporations, criminal syndicates and other non-state actors. Furthermore, adversaries now employ methodologies, tradecraft and collection techniques virtually unknown a decade ago, particularly in the areas of computer network attack and exploitation.

Handbook Strategy and Use

"CI and Op Sec" planning is a must in order to protect information and vital assets from theft, espionage and unauthorized disclosure. This handbook was developed for a target audience of junior and mid-level government, business and industrial managers and security planners needing a practical introduction to counterintelligence and operational security planning. A key goal is to assist leaders in understanding the nature of the threat, increasing organizational awareness, and implementing effective protective strategies and countermeasures.

Must Do

The nature of current threats has increased the necessity for all government, business and industry leaders to possess a basic familiarity of counterintelligence practice and operational security.

The handbook provides an introduction to the field of counterintelligence and security planning; key concepts and terms; an overview of organizations and functions comprising the U.S. counterintelligence community; and private sector resources for training and education. The handbook introduces a six-step approach for counterintelligence and operational security planning. The concise and organized methodology emphasizes integrated functions of physical, personnel and information security. The process also provides basic strategies for conducting vulnerability assessment, risk management functions, asset protection planning, countermeasure development, operational security best practices, and development of training and education programs.

Key Focus Areas

Introduction to counterintelligence discipline, organizations and functions.

- Basic terms, definitions and organizational structure of the government's counterintelligence and security apparatus.
- Overview of current threats from foreign intelligence services, including emerging trends, key actors, collection methodologies and indicators.
- Introduction of a six-step process for organizational counterintelligence and operational security planning.
- Countermeasures and risk management strategies for protecting people, facilities and information.

- Templates for developing counterintelligence and security awareness, training and educational programs.
- Counterintelligence and security best practices for protecting people, facilities and information.
- Resource and reference guide to counterintelligence and operational security topics.

Introducing Counterintelligence and Operational Security

“Nowadays counterintelligence is no longer a government problem. It’s a problem for any firm that has valuable secrets to keep, regardless of whether those secrets may be classified.”[10]

Defining Counterintelligence

The term “counterintelligence” is often misunderstood, in part because the discipline encompasses a range of varied activities. By its most basic definition counterintelligence involves activities designed to detect and prevent espionage by countering an adversary’s intelligence operations and intentions. Even within this narrow understanding is implied a wide range of tasks, functions and operations. Many CI efforts overlap with other disciplines such as: foreign intelligence collection; personnel, physical, information and cyber security; force protection; operational security; counterespionage; law enforcement investigation and counterterrorism. A certain degree of debate exists among seasoned intelligence and security practitioners as to the precise lines of demarcation between the field of counterintelligence and the many integrated supporting and complementary functions.

Remember

As a basic starting point, counterintelligence may be understood as activities designed to protect classified or sensitive information, intelligence operations, military technology, diplomatic activities, and business or economic information relating to national security matters.

More broadly, counterintelligence focuses on identifying an adversary’s intelligence collection capabilities, methodologies and targets, and also taking action to neutralize or mitigate those threats. Specifically, the Office of the National Counterintelligence Executive (NCIX) defines counterintelligence as “the business of identifying and dealing with foreign intelligence threats to the United States. Its core concern is the intelligence services of foreign states and similar organizations of non-state actors, such as transnational terrorist groups. Counterintelligence has both a defensive mission – protecting the nation's secrets and assets against foreign intelligence penetration – and an offensive mission – finding out what foreign intelligence organizations are planning to better defeat their aims."[11]

Clearly the scope of counterintelligence operations varies significantly from one organization to another depending on the entity's structure, mission and purpose. For instance, military counterintelligence traditionally focuses on identifying and countering espionage threats by hostile intelligence services or adversaries engaged in acts of sabotage, subversion or terrorism against military forces. However, military CI also plays a role in physical security and force protection, and activities designed to deny an adversary access to information, particularly about potential force vulnerabilities. In today's era of diminished privacy and a generational swing toward consummate openness, military CI could entail something as simple as educating young troops about the danger in posting information – regarding physical location, psychological status or emotional mindset – on social networks such as Facebook and MySpace, which invariably lack security.

> For a business executive or industrial security manager, counterintelligence has a somewhat different focus, one more concerned with detecting and preventing industrial espionage, guarding against critical information loss, theft of proprietary technology or ensuring supply chain integrity.

Private sector counterintelligence may also focus on such concerns as protecting internal businesses information, secrets relating to merger and acquisitions, guarding product prototype design, or securing marketing strategies from competitors. Since private sector employees often are not trained to be as security-conscious as the government workforce or military troops, corporate CI requires raising workforce awareness about potential threats and implementing secure practices. The number of employees who telecommute or work remotely – often at locations utterly void of security, such as Internet cafes, airport lounges, trains and commuter rails – presents an additional CI challenge for businesses.

Another example is the counterintelligence role of the FBI and intelligence community, whose focus emphasizes analysis to determine how an adversary collects information as well as investigations and operations to detect, block and disrupt such efforts.

Adding to the confusion are philosophical debates as to whether counterintelligence is primarily an intelligence function – with emphasis on analysis and collection – or a law enforcement activity focused on investigation, evidentiary procedure and legal principles. Even counterintelligence functions within the Department of Defense (DoD) and military services reflect this debate: the Army aligns its counterintelligence mission with human intelligence activities, while the Navy and Air