

SECURITY IS
EVERYONE'S
BUSINESS

Security Times

VOLUME 3 SECURITY BRIEFING

01 MAY 2008

Threat Awareness 1

Defense Security 1

Security Classification System 2

Employee Reporting Obligation & Requirements 3

Security Procedures / Duties 3

Security Tips & Reminders 3

About COLE Technology Corporation 4

INSIDE THIS
ISSUE:

SECURITY
BRIEFING

Threat Awareness

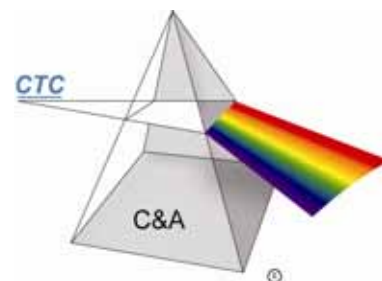
The success of the overall Department of Defense (DoD) mission is, in part, dependent upon the security practices and procedures established by contractors. The following areas are briefly discussed to ensure COLE Technology Corporation's compliance, by instituting and maintaining appropriate security practices.

The area of information technology is under constant threat of being targeted by industrial and foreign intelligence services. U.S. industry develops, produces or works with the majority of our nation's technology,

much of which is sensitive an classified – and thus plays a significant role in creating and protecting the information that is so vital to our National Security. The requirement to protect sensitive and classified information is imposed as part of our contractual obligation to our clients.

The objective of industrial security is to ensure that security systems are established and maintained to deter and detect espionage, and to counter the threat posed by traditional and nontraditional adversaries who target sensitive and classified information. Cost-effective measures

must be established and applied to counter identified risks. The National Industrial Security Program Operating Manual (NISPOM), maintained by the Facility Security Officer (FSO), provides guidelines for developing a defensive security posture within the organization. General guidelines are outlined within this briefing.



Defensive Security

You are responsible as an individual for protecting and safeguarding sensitive and classified information at all times, both on and off the job. This responsibility continues after your employment with COLE Technology Corporation terminates. Your responsibilities are real – they are magnified as a

result of your employment in a vital defense industry. It is essential that you realize the importance of this and act appropriately. Unauthorized disclosure or failure to properly safeguard sensitive and classified information is punishable under Espionage Laws and Federal Criminal Statutes.

This initial security briefing is provided to you in written format for your continued reference, and to emphasize the importance of following security guidelines. This initial security briefing will be supplemented by annual refresher briefs and other required follow-ups to (Continued on page 2)

Defense Security Continued



reinforce important aspects of security and to inform you of changes in security regulations. These refresher briefings may include relevant and current news articles that deal with espionage and security problems within the industry.

Any security related questions should be addressed to your Facility Security Officer (FSO) at the corporate headquarters in Fort Worth, TX:

Jeremy A. Cole
(817) 320-2934
jacole@ctc-coleassociates.com
Threat Awareness Specialist

“Classified material should be clearly marked, so that there is no doubt as to the classification of the material”

The Security Classification System

What is classified material? Information is classified when it is determined that its unauthorized disclosure can reasonably be expected to cause some damage to national security. If this is the case, the material is assigned the classification of TOP SECRET, SECRET, or CONFIDENTIAL. Unauthorized disclosure means disclosure to someone not authorized by the Government to have access to classified information. Unauthorized disclosure is punishable as detailed in the Extracts of the Espionage and Sabotage Acts.

Determining access to classified material? When an individual is granted a security clearance by the proper

authority, it means that an individual is eligible to have access to classified information on a “need-to-know” basis. Access is granted only when the following two conditions are met:

1. The recipient has a valid and current security clearance at least as high as the information to be released. Contact your FSO if in doubt about a person’s clearance status, AND
2. The recipient requires access in order to perform tasks essential to the fulfillment of a classified Government contract or program. This is called “need-to-know.” Contact the recipient’s supervisor if in doubt about a person’s “need-to-know.”

the possessor of classified information to ensure that the prospective recipient meets BOTH of these conditions.

How do I know if it’s classified? Classified material should be clearly marked, so that there is no doubt as to the classification of the material. These markings show the highest classification on the page at the top and bottom of each page, and each portion and title is marked to indicate their individual classification. The Government or prime contractor furnishes classification guidance, which specifies the proper classification to be assigned.



It is the responsibility of

Reporting Obligations / Requirements

General - It is the personal responsibility of each employee to observe all security regulations. You must report the following information to the site Security Officer, where the incident occurs, and to your FSO:

- Any loss, compromise, or suspected compromise of classified information
- Any information regarding existing or threatened

espionage, sabotage or subversive activity within the company or Government worksite

- Anyone attempting to solicit classified or proprietary information who is unauthorized to do so
- Any classified material made accessible to you
- Before you receive a clearance
- Suspicious Contacts

- Information regarding the status of citizenship by naturalization
- Any threats to company security
- Any theft of Government property
- Changes in Personal Status
- Business-Related Visits
- Attendance at Conventions, Trade Shows, Symposiums

“All COLE Technology Corporation Employees

will adhere to the policies and procedures at their respective places of work”

Security Procedures / Duties

COLE Technology Corporation maintains a TOP SECRET facility clearance; however, no classified information is contained at the headquarters office. All classified information is maintained at respective Government sites where COLE has contracts.

All COLE Technology Corporation employees will adhere to the policies and procedures at their respective places of work at Government sites. This specifically includes all

regulations and security practices regarding the marking, handling, and safeguarding of classified information. This may also include, but is not limited to, procedures regarding computer passwords and other automated information security safeguards. All security questions related to a specific work site should be addressed to the respective site Security Officer (usually, a Government representative).

Security clearances are

granted to individuals based on the needs of specific contracts. The expansion and contraction of Government requirements may cause changes in an individual’s need for a particular security clearance.

Debriefings are provided upon termination of employment, when an individual’s security clearance is suspended or terminated, or when the facility clearance is terminated.

Security Tips & Reminders

- Safeguard classified material at all times
- Do not discuss classified information over the phone
- Store all classified material properly
- Check your desktop, file drawers, tabletops, etc., before departing from your work area. Also lock files and safes before you leave
- Ask your supervisor or Security Officer when in doubt about security regulations
- Make sure classified material is properly marked and identified
- Use the proper covers on all classified material

- Don’t reveal or permit access to classified information to employees or persons who do not have the proper security clearance AND the “need-to-know.”

**SAFEGUARD
CLASSIFIED
MATERIAL
AT ALL TIMES**





Department of Defense
HOTLINE
 for reporting fraud, waste, and abuse
1-800-424-9098

About COLE Technology Corporation

COLE Technology Corporation is a professional services company operating nationally since 1998 to deliver comprehensive consulting, training and program management services to a broad range of Department of Defense, Government, Industry, and Educational institutions in five primary focus areas of consulting.

- Management and Organizational Business Improvement Systems and Services
- Infrastructure and Resources Planning and Management
- Intelligence Analysis
- Threat Awareness, Indications and Warning Security
- Continuity of Operations Programs and Emergency Relocation Sites

We are a cadre of highly trained and experienced consulting professionals, with extensive background and experience in Military and Government Infrastructure and Resources Management, in Military and Law Enforcement Intelligence and Security, Intelligence, Information Technology, Homeland Security and Counter-Terrorism. The skills and resources of our corporation span a broad spectrum of Military and Government planning and management, and intelligence training and consulting capabilities, with our associates and contract work projects located throughout the nation.

COLE Technology Corporation is certified by the General Services Administration as a

Service Disabled Veteran-Owned Small Business with a MOBIS (Mission Oriented Business Integrated Services) Schedule. Our services may be obtained under the GSA Schedule in the following areas:

- Business Operations / Strategic Planning
- Facilities / Operations / Management
- Infrastructure / Emerging Technology
- Resources Management / Programming
- Program Management / Project Management
- BRAC, COOP, ERS Contingency Programs / Planning / Analysis
- Intelligence Programs Management
- Threat Analysis / Threat Awareness Programs and Training



For more information, please visit
www.ctc-coleassociates.com

COLE Technology Corporation
4500 Mercantile Plaza Dr. Suite 230
Fort Worth, TX 76137
Phone: (817) 320-2934
Fax: (817) 546-9884
www.ctc-coleassociates.com

