Consultant
Annual DoD Security Refresher
About This Course

• This course should be taken by Consultants Only in this PDF format
  – All others should take this course online
    • LMPeople > LMCareers > Learning and Development > Learner’s Desktop, then select the Learning Plan tab
• The content of this course fulfills the requirements for both a DoD clearance and an SCI access. If you hold both, taking this course will fulfill one requirement and may waive the other on your learning plan. For further information check with your local Security Representative
Course Objectives

• Upon completion of this course, you will refresh your knowledge in the following areas:
  • CI/Threat Awareness
  • Physical Security
  • Information Protection
  • Personnel Security
I’m Robert Trono, Vice President and Chief Security Officer at Lockheed Martin. I’d like to welcome you to your annual Security Refresher briefing.

If I were to ask you, “Who is responsible for security?” how would you answer?

I hope that each of you would answer that you are responsible because, as a cleared U.S. citizen and Lockheed Martin cleared Consultant, you serve as a vital member of our security team each and every day.

You play a critical role in protecting classified information and following other security requirements. Our corporation continues to expand into the global arena, and the landscape of our business is changing. This evolution brings with it new security challenges.

The threats to our resources and information continue to emerge and proliferate. Some threats are in the cyber arena, including spear-phishing, viruses and malware. Others are more traditional, such as theft and foreign and economic espionage.

It is vital that you are alert to both the technical and non-technical threats and familiar with the protective measures you can take. Additionally, it is important to be aware of the policies and processes in place to ensure we remain compliant with government regulations concerning the protection of classified information.

This annual briefing was developed to increase your awareness and sharpen your security skills while you serve as an integral member of our security team. If you have any questions about the material covered in this module or any other security concerns, please contact your local Security Representative immediately.

Thank you for paying close attention to the upcoming refresher module, and thank you for your continued diligence in your security responsibilities.
Counterintelligence/Threat Awareness
Key Points To Remember

• The best way to counter threats is to know the targets, know your adversaries, know how to protect and report information and always report any suspicious information activity or attempts to obtain information

• Counterintelligence consists of the actions we take to counter adversary intelligence, espionage and sabotage efforts

• Counterintelligence protects classified and sensitive information

• Collection threats come from many places; foreign governments, competitors, and even trusted insiders (e.g. a coworker)
• Every year billions of dollars are lost to foreign and domestic competitors who exploit open source, sensitive and classified information

• You are the frontline of defense against these threats. Being alert to the threat and reporting any suspicious activity contributes to helping Lockheed Martin maintain its competitive advantages and our national security
Possible Collection Methodologies

• Requests for Information
  • This is the most frequently reported collection method and provides the greatest return for minimal investment and risk. Collectors use direct and indirect requests for information (e.g. e-mails, phone calls, conversations) in their attempts to obtain valuable U.S. data. These types of approaches often include requests for classified, sensitive, or export-controlled information. A simple request can net a piece of information helpful in uncovering a larger set of facts
Possible Collection Methodologies

• Solicitation or Marketing of Services
  • Foreign-owned companies seek business relationships with U.S. firms that enable them to gain access to sensitive or classified information, technologies, or projects

• Acquisition of Technology
  • Collectors continue to exploit direct and indirect acquisition of technology and information via third parties, the use of front companies, and the direct purchase of U.S. firms or technologies

• Public Venues
  • Conferences, conventions, symposiums and trade shows offer opportunities for foreign adversaries to gain access to U.S. information and experts in dual-use and sensitive technologies
Possible Collection Methodologies

- Official Foreign Visitors and Exploitation of Joint Research
  - Foreign government organizations, including intelligence and security services, consistently target and collect information through official contacts and visits

- Cyber Attack
  - Cyber threats are increasingly persistent and rapidly becoming a primary means of obtaining economic and technical information. Reports of new cyber attacks against U.S. government and business entities continue to increase. Adversaries have expanded their computer network operations, and the use of new venues for intrusions has increased

- Mobile Telephones
  - Threats against mobile phones continue to rise. Smart phones such as Blackberry and iPhone, essentially general purpose computers, are susceptible to malicious software, according to open source reporting
Foreign Targeting of U.S. Travelers Overseas
- Foreign collectors also target U.S. travelers overseas. Collection methods include everything from eliciting information during seemingly innocuous conversations, to eavesdropping on private telephone conversations, to downloading information from laptops or other digital storage devices.

Targeted Information and Sectors
- Foreign collectors continue to seek a wide range of unclassified and classified information and technologies from specific targets. Information systems attract the most attention; aeronautics, lasers and optics, sensors, and marine systems are other top targets.
Report Suspicious Activity

Elicitation attempts
Espionage
Terrorism/Sabotage
Any suspicious contacts

• To counter these threats, it is important to report these items

• Any vulnerability, no matter how seemingly inconsequential, should be reported to your Security Representative as soon as possible

• Our company works with law enforcement and government agencies to counter the threat
OPSEC

• In addition to knowing the methodologies and when to report, it is also important to know about OPSEC

  • Operations Security (OPSEC) – when we deny adversaries any information about capabilities and/or intentions. This means we need to identify, control, and protect generally unclassified information related to sensitive activities so that we can reduce vulnerabilities to our information
Targets: Cell Phones

• In addition to data on computers, know that adversaries are targeting devices such as smart phones, MP3 players, and mini notebooks to steal trade secrets, sensitive and economic information.

• Vulnerabilities include:
  • Text messages
  • Blue tooth
  • Applications
  • GPS

• Check with your Information Systems Security Officer (ISSO) or Information Systems Security Manager (ISSM) to make sure you understand the rules regarding what devices are permitted into your area or for use on your programs, and to what extent such a device can be used outside a classified workspace.
Physical Security
Key Physical Security Components

- Securing the area
- Office set-up (e.g. computer and phone placement)
- Visitors
- Badges
Key Points to Remember

• If you work in a classified area, the area is secured at the end of the day. It may need to be opened each day in a similar method
  • Some offices have spin locks, cipher locks and/or card readers
  • Sometimes there is an individual who acts as a “monitor”

• End-of-day checks require internal lock up procedures on computers and safes

• Each of us is responsible for securing our own information and workspace
  • Part of securing your workspace is compliance with requirements for physical security
Key Points to Remember

• The reason telecommunications and computer systems are separate is to prevent classified data from being released into an unclassified environment

• If you have questions you may always ask your Security Representative
Visitors

- It is the host’s responsibility to verify that their visitors have the appropriate clearance and “Need-to-Know”

- If visitors are cleared, it is possible that paperwork may need to be coordinated with Security prior to the visit. It is also possible that their clearance data is available in a security database. Ensure that everything is settled prior to the visitor’s arrival

- While in Lockheed Martin facilities, visitors must be correctly badged with that facility’s proper credentials and escorted if necessary
Badges

- When used in conjunction with a card reader to access Lockheed Martin facilities, the badge represents the first line of defense in protecting against unauthorized intrusions
- Report any badge issues to Security as soon as they occur
Badges

• Protection
  • In the community, don’t give people the opportunity to see your credentials and identify you as a Consultant. It can make you a target for solicitation and social engineering, and may indicate where employees and/or Consultants frequent afterhours. This information is helpful to those seeking our data

• Storage
  • When you leave the facility, remove your badge and put it in a safe place with low visibility

• Purpose
  • The badge is intended to strengthen our personnel, asset, and information protection capabilities as well as enable ready identification of people on our premises

• Display
  • When at Lockheed Martin facilities, your Lockheed Martin badge, by corporate policy, needs to be worn in plain sight, between the shoulders and the waist on your outermost garment
Information Protection
Key Points to Remember

• Protecting both classified and unclassified information is important

• A type of unclassified information that warrants protection is proprietary information

• Publication of classified information does not necessarily mean it has been declassified – this information has been leaked into the media in the past and has caused grave damage to national security
Proprietary Information

• Lockheed Martin Proprietary Information
  • Information unique to Lockheed Martin

• Third party or export controlled information
  • Comprises new technologies and innovations including engineering designs, computer code, financial data and customer data

Note: Use caution when revealing details regarding program names, technology, mission, locations, cost and research and development activities
Secure Communications

• When in doubt, use secure communications

• Phone and computer
  • Open and secure communications are available. Prior to making a call or starting a file, take a moment to ensure you are using the right system for your work

• Compilation
  • Ensure that when combining unclassified terms, emails, items, etc. it won’t turn into classified information

• Destruction
  • Sensitive information should be destroyed in a designated manner that precludes its reconstruction, such as shredding, burning or other measures. There are customer specific guidelines for the destruction of classified information. Check with your Security Representative for specific guidance
Secure Communications

• Live Conversations
  • You do not have to be in a secure area to discuss proprietary information.
  • You should try for as much privacy as possible and do not conduct sensitive conversations in public locations or open areas. Ensure all parties have a Need-to-Know and that you are protecting the information as well as you can.
Classified Materials

• Except in connection with authorized visits:
  – You shall not possess classified material away from the premises of Lockheed Martin Corporation
  – No classified material will be physically removed from any Lockheed Martin facilities, other contractor facilities or User Agency facilities, by a Consultant for any reason, except in connection with authorized visits
  – Lockheed Martin Corporation shall not furnish classified material to Consultants at any location other than the premises of Lockheed Martin Corporation
  – Consultants shall perform classified elements of the consulting services only on the premises of Lockheed Martin Corporation

• Lockheed Martin Corporation shall provide classification guidance to Consultants and shall brief the Consultant as to the security controls and procedures applicable to the Consultant’s performance
Classification Markings

• Classification markings are used on everything from casual meeting notes to formal proposals and media

• These markings identify the information which requires protection and to what level it’s protected

  • Confidential
  • Secret
  • Top Secret
Classification Markings

- Markings on the top and bottom of pages are required to let the readers know the information they are reading is classified.
- Paragraph or portion marks individually label sections of information with their appropriate classification level.
- Markings may also detail origin of classification, safeguarding requirements and dissemination controls.

Note: Customers may have their own guidelines on how they want documents to be marked.
Two Types of Classification

Original Classification
An initial determination made only by U.S. government officials

Derivative Classification
The responsibility of contractors who incorporate, restate, or generate in new form, information which is already classified by the U.S. government

Contact your Security Representative/Facility Security Officer (FSO) for derivative classification guidance
Need-to-Know

• Need-to-Know is another way to protect information

• It prevents unauthorized disclosure of classified information. It states that even if a person has a clearance, you should not share information that you are protecting with them if they do not have a “Need-to-Know” the information
Non-disclosure Agreement

- Should you reveal classified information to an unauthorized person, you will be liable under the non-disclosure agreement.

- The penalties for violating U.S. Code are severe and may include the loss of accesses, termination of position, fines, and imprisonment.

- If you signed the agreement you are required to submit any information that is planned for public release to pre-publication review to ensure no disclosure of classified, proprietary or FOUO information is found.

- For guidance on the review process you may contact your Security Representative.

- Sometimes relationships and associations on classified contracts are not for publication.
Public Networks

• Be cautious in what you reveal about your job in online forums, such as blogs, wikis, message boards and social networking sites. Even hinting or alluding to the fact that you have access to classified information can make you a target for solicitation, viruses and malicious code.

• If you are SCI-briefed you must also have your resume reviewed prior to publication.
Example Resumes

GOOD RESUME

• Completed a Single Scope Background Investigation (SSBI), July 2008

• Cleared DoD Top Secret

• Successful completion of a government polygraph

• Granted Access to Sensitive Compartment Information by U.S. government

BAD RESUME

• Participated in program mission to provide customer with advanced subterranean radar technology

• Cleared on the NAQ compartment

• Cleared to work with BORA information

• Worked with Iguana Cord program for Department of Homeland Security
Personnel Security
Reporting Requirements

- The government has established a number of reporting requirements to maintain our access to classified information
- Reports cover areas that are considered personal vulnerabilities, such as finances, relationships, loyalty, lawfulness, etc.
- The government wants you to be up front and report, so a foreign agent can’t take advantage of the vulnerability and exploit it
- Reports are private and security professionals hold this information in the highest confidentiality
- You may be required to report some or all of the following: home address, phone number, name and citizenship
DoD Access Reporting Requirements

• Representation of a foreign interest- Report your affiliation with foreign government, an agency of a foreign government, or representative of a foreign government, any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the U.S. or its possessions and trust territories, and any person who is not a U.S. citizen or national of the U.S.

• Foreign Travel- Report only on periodic update paperwork. Recommend keeping track of trips for your own information

• Suspicious Contact- Report any contact, domestic or foreign, that is suspicious in nature. Contacts can occur online, via phone, written correspondence or in person

• Adverse Information- Report anything you observe in yourself or another’s conduct or character that could affect his/her ability to protect classified information
SCI Access Reporting Requirements

• Foreign Travel- Travel outside the U.S. must be reported using the Pre- and Post-Travel forms or via Personnel Security. Some customers may have additional requirements. Call your appropriate Foreign Travel Representative to verify the need for training.

• Foreign Contacts- You must report all contacts of the following nature:
  • Contacts involving bonds of affection, personal obligation, or the exchange of personal or business information
  • Sexual liaison
  • Joint business or financial relationships
  • Foreign national interest in classified, proprietary, or export-controlled information or inquiries about an individual’s access to classified information or operations
SCI Access Reporting Requirements

• Foreign Contacts (cont’d):
  • Individual concern about undue or unsolicited interest in personal or professional activities by a foreign national
  • Foreign nationals affiliated with a foreign government, e.g. military
  • Foreign national’s unsupervised access to an individual’s residence (exception: maintenance or service personnel who may have non-recurring access)
How to Report Required Information

• Required Information may be reported in one of two ways:

• Send the information details to requiredreports.lmsecurity@lmco.com

• Report the information to your local FSO who will then send the information to LMSecurity
Course Completion

• Please note: You as a Consultant represent Lockheed Martin. If you have access to Classified information you are to contact Lockheed immediately upon termination of contract or any other changes regarding your representation.

• Thank you for completing your Annual DoD Refresher Briefing.

• In order to receive credit for taking this course please follow the instructions on the next slide.
To Take Credit for This Course (Consultants Only)

• Consultants Only (all other employees will receive credit automatically once completing the course online): To acknowledge that you have taken this course please follow the below instructions:

  • Complete and input this phrase into an email:
    • I (input your name) acknowledge that I have reviewed and completed my DoD Annual Refresher Briefing in its entirety on this date (input date completed mm/dd/yyyy).

  • Send the email to your local FSO and Clearances.Lmsecurity@lmco.com on the same day of completion of the course.