DoD Initial Briefing

LOCKHEED MARTIN

Overview

- **Lockheed Martin plays a direct role in our nation's defense. Our technical systems and solutions are among the finest ever created, enabling the United States to prevail over adversaries while protecting allies**

- **The U.S. Government has established several safeguarding methods to ensure the protection of its secrets. You have been approved for access to classified Department of Defense (DoD) collateral information.**

- **This course is intended for employees who have just been granted their DoD Security Clearance. This includes employees who have been granted their clearance for the first time or are transferring in with a previously granted clearance (prior military and/or other DoD contractor)**

Overview

- In this course, we'll explore a variety of standard security procedures that are critical for employees with DoD clearances to understand and follow
- Although each cleared LM facility adheres to set government security standards, implementation procedures may vary from site to site. This is often due to specific customer requirements, physical building characteristics, etc
- Your local security representative will be able to direct you to local standard process procedures and provide additional program specific information

Overview

- **Lockheed Martin employees are required to protect all classified information to which they have access and/or custody. By holding a security clearance granted by the U.S. Government, you have the responsibility of safeguarding classified information at all times, both on and off the job. Classified information is information or material that has a direct bearing on the national defense of the United States**
- **The security concepts in this briefing provide the detailed requirements as defined by the National Industrial Security Program Operating Manual (NISPOM). These requirements provide the guidance necessary to protect our nation's secrets**

The protection of classified information is a lifelong obligation

Overview

- **Upon completion of this course, you will be able to:**
  - **Describe threat awareness**
  - **Be aware of Operations Security (OPSEC) threats and conditions**
  - **Understand your reporting requirements**
  - **Define security concepts**
  - **Explain the concepts of a security clearance and Need-to-Know**
  - **Understand classified information handling**
  - **Identify the requirements for processing classified information on a computer system**
  - **Understand Communications Security (COMSEC)**
  - **Understand the Visit Request process**
  - **Describe proper travel procedures**
  - **Be familiar with LMSecurity and understand its value in the corporation**

Threat Awareness & Defensive Security Measures

Threat Awareness and Defensive Security Measures

- **As the world's leading defense contractor, Lockheed Martin continues to be a target for intelligence collectors and terrorists around the globe**
- **Threats are unpredictable because they come from within AND outside of our borders, from hostile and friendly countries alike**
- **In order to prevent classified information from falling into the wrong hands, all employees must understand that security threats do exist and must be aware of the dangers that those threats pose to our company and our nation**
- **It is important that you understand that espionage is not easily distinguishable. In this day and age, it is very difficult to determine who the "good guys" are**

Threat Awareness and Defensive Security Measures

Stringent and well-enforced security measures have done a lot to keep outsiders from looking in, but insiders can and often do present an even greater threat. Americans and others living in this country have committed espionage for any number of reasons. There are a variety of motivational factors that lead to a person's decision to compromise classified information. Some of these factors are:

Money

Ideology

Coercion

Ego

Threat Awareness and Defensive Security Measures

- **In the realm of espionage, things are not always as they appear. We need to be aware of seemingly harmless behaviors and acknowledge any obvious "red flags" that should serve as a warning to potential problems**
- **Some "red flags" can include:**
  - **Sudden or unexplained affluence**
  - **Odd working hours**
  - **Excessive copying of classified or proprietary data**
  - **Carrying packages in and out of the buildings**
  - **Unwarranted questions**

Threat Awareness and Defensive Security Measures

One of the most recent cases of espionage involved an individual by the name of Robert Hanssen

Robert Philip Hanssen was an FBI agent who was convicted of spying for the former Soviet Union. He was arrested on February 20, 2001 at a park near his home in Vienna, VA and charged with selling American secrets to Moscow for $1.4 million in cash and diamonds over a 15-year period. His treason has been described as the "worst intelligence disaster in US history."

Operations Security (OPSEC)

Operations Security (OPSEC)

- **OPSEC, or Operations Security, is a process of identifying, controlling and protecting generally unclassified information which, if it becomes known to a competitor or adversary, could be used to our nation's and country's disadvantage. OPSEC does not replace other security disciplines – it supplements them**
- **The United States has suffered several terrorist attacks in recent years. In many of these cases, the terrorists were successful because they knew our vulnerabilities**
- **Since Lockheed Martin is the world's largest defense contractor, it is important that employees recognize there is a chance they could become the target of one of these terrorist acts. By incorporating OPSEC into our everyday work routine, these risks are lowered significantly**

Operations Security (OPSEC)

- **The OPSEC process is a risk management instrument that enables the individual to view an operation or activity from the perspective of an adversary**
- **One should ask oneself, "What information do I need to know to thwart an adversary's unsavory intentions and actions, and how might an adversary attempt to gather the information he or she needs?"**
- **In the simplest terms, to practice OPSEC is to know what information our adversaries are looking for – and withhold it from them. It means stepping outside ourselves and looking at whatever we're working on through the eyes of our adversaries. Good OPSEC includes knowing that the collection of unclassified data could give away key classified data**

One of the most important responsibilities you have as a cleared employee is to report suspicious activity

Department of Defense Hotline

To report fraud, waste or abuse, please contact your local security office. If you do not feel comfortable informing Lockheed Martin, call the Department of Defense Hotline at 1-800-424-9098.

Reporting Requirements

Reporting Requirements

- **It is your responsibility as a cleared employee to report information that suggests your ability (or that of a co-worker) to safeguard classified information may be impaired**
- **Adverse Information is anything that may bring into question a person's ability to safeguard classified or sensitive data**

Adverse information should be reported via your local Facility Security Officer (FSO) or by email to requiredreports.lmsecurity@lmco.com

Reportable Adverse Information

- **Some examples of reportable adverse information are as follows:**
  - **Inability to safeguard classified information (disregard for security procedures, intentional unauthorized disclosure, etc.)**
  - **Deliberate falsification of security clearance package information**
  - **Foreign influence (obtaining a foreign passport, ownership of foreign property, marriage or cohabitation with a non U.S. Citizen)**
  - **Disloyalty to the U.S. (acts of sabotage, espionage, or subversive activity)**
  - **Misuse of information technology systems, including the downloading of unauthorized information**
  - **Criminal activity of any kind, including detainment or arrest**

Reportable Adverse Information

- **More examples of reportable adverse information are as follows:**
  - **Dishonest conduct**
  - **Erratic behavior, emotional problems**
  - **Excessive indebtedness or recurring financial difficulties (i.e., bankruptcy, wage garnishment, repossession, liens placed on personal property for failure to pay taxes, etc.)**
  - **Unexplained affluence**
  - **Excessive use of intoxicants (alcohol abuse, substance abuse, or chemical dependency affecting job performance, including that which involves legally prescribed drugs)**

Additional Reporting Requirements

- **Besides adverse information, there are additional reporting requirements when there are changes in your personal status**
- **You are required to report the following items:**
  - **Legal name change**
  - **Marriage**
  - **Divorce**
  - **Cohabitation in a spouse-like relationship**
  - **Changes in citizenship**
  - **Your representation of a foreign interest**
  - **Contact you may have with someone who asks suspicious questions**

Additional Reporting Requirements

- **All reporting requirements can be reported to your local FSO or you may send it via email to requiredreports.lmsecurity@lmco.com**
- **You are protecting yourself, your co-workers, and our national security by reporting this information**

Security Concepts

Classification Markings

- **There are three levels of U.S. classified information:**
  - **Confidential (C) - unauthorized disclosure can cause “damage” to National Security**
  - **Secret (S) - if divulged, can cause “serious damage” to National Security**
  - **Top Secret (TS) - if disclosed, can cause “exceptionally grave damage” to National Security**

Need-to-Know

- **Only the U.S. Government can classify information. The most common sources of classified information are:**
  - **Technical specifications**
  - **Threat documents**
  - **Communications**
  - **Mechanical components**
- **Before classified material is disclosed, the individual must have the proper clearance and must have a "Need-to-Know." Remember, rank, level, or position within the company does not equal a Need-to-Know. If you have a question about with whom you should share classified information, ask your local security representative**
- **Regardless of the classification, treat all classified information with the utmost discretion and care**

Classified Information

Classified Materials

- **Classified material must ALWAYS be safeguarded. Some general requirements include:**
  - **Never leave classified material unattended**
  - **Must be secured in a government approved container or left in the personal custody of a cleared employee with appropriate clearance level and the Need-to-Know**
  - **Properly secure classified materials when you leave for the day**
  - **In case of an emergency, all practical security measures should be followed for safeguarding classified material as the situation allows; however, employee safety comes first**

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 an employee for any reason, except in connection with authorized visits**
- **Lockheed Martin Corporation shall provide classification guidance to our employees and shall brief them as to the security controls and procedures applicable to their performance**

Classified Materials

- There are severe penalties for knowingly and willfully disclosing classified information
- There are penalties for disclosing classified information through negligence, including lack of knowledge concerning the proper handling of classified information

Ignorance is NO excuse. Penalties include a fine of up to $10,000, imprisonment of up to 10 years, or both

Classified Information: Classified Documents

- **The highest level of classified information contained within a document determines its overall classification marking. Physically marking classified information with one of the classification levels serves as a warning to the degree of protection required to safeguard it**
- **Classified documents are required to be marked in accordance with government guidelines. These guidelines are contained in marking guides available to you. Contact your local security representative for more information**

Classified Information: Working Papers

- **Working papers such as notes, sketches, and rough drafts should be dated when created, marked with appropriate levels of classification, and annotated “WORKING PAPERS"**
- **Working papers retained for more than 180 days or those transmitted outside of the facility must be marked in the same manner as prescribed for a finished document**
- **As older drafts become redundant, they should be destroyed in accordance with local destruction procedures**

Classified Information: Reproduction

- **The reproduction of classified material should be kept to a minimum**
- **Please see your local security office for the site specific policies and procedures regarding the reproduction of classified information**
- **When copies are made, the new document must be marked with the same classification marking as the original**

For more information check with your local security representative for instructions

Classified Information: Hand Carry

- **The hand carrying of classified information should only be used as a last resort. Approved hand carriers must:**
  - **Receive a thorough briefing from their local security representative in hand carry requirements**
  - **Possess an approved photo identification card**
  - **Keep the materials in their possession at ALL TIMES**
- **It is the employee's responsibility to ensure that the intended recipient AND the recipient's location have the proper clearances, safeguarding capability, and Need-to-Know before sharing any information marked as "classified"**

For More Information check with your local security representative for instructions

Classified Information: Receipt and Transmittal

- **Classified information that can be released or exchanged in various formats must follow the guidelines defined in the NISPOM**
- **All classified documents received at a facility must pass through the authorized local security representative prior to being delivered to an employee**
- **Never have classified material sent directly to your building address**
- **Your local security representative must be contacted prior to the transmittal of classified information**
- **If you receive a classified package directly, notify your local security representative IMMEDIATELY**

Classified Information: Final Thoughts

- **At Lockheed Martin it is not only your privilege, but your duty to handle our country's most sensitive secrets and cutting edge technologies in a very responsible manner**
- **In addition to the requirements for handling hardcopy and physical classified information, there are also special requirements for dealing with computer systems on which classified information is processed; as well as when handling electronic versions of classified information**

Classified Information Systems

Classified Information Systems

- **A classified Information System (IS) typically consists of computer hardware, software, and/or firmware configured to collect, create, communicate, transmit, process, store, and/or control data or information**
- **As more and more information is processed electronically, protecting our information systems (computers, their users, and computer networks) requires a balanced approach that includes computer-specific features as well as administrative, operation, physical and personnel controls**
- **The Information Systems Security Manager (ISSM) is responsible for the administration of all DoD classified processing**
- **Prior to processing or accessing any classified information, you must fully understand the Information Systems Security Plan (ISSP)**

Classified IS: Know the Requirements

- **Ensure that you are fully briefed on all security requirements by your ISSM**
- **You must protect your passwords to the highest classification level of the system you are using them on, and you are not permitted to share them**
- **An individual's password must be changed whenever there is a suspicion that the password has been compromised. Also, when the user no longer has a Need-to-Know or the proper clearance for the system, their account must be disabled**
- **A classified computer must never be connected to or share information with an unclassified computer. This includes home computers, personal laptop or other personal devices such as Personal Digital Assistants and the like**

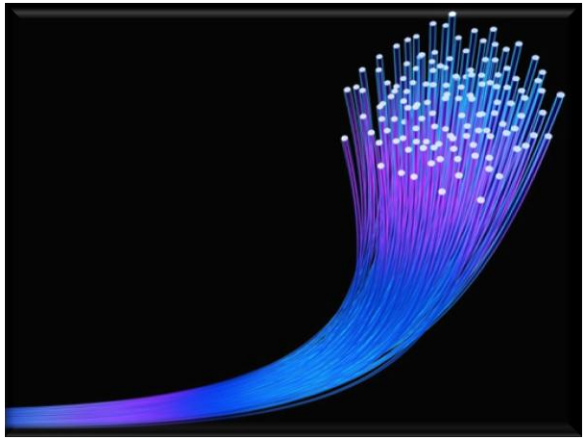
Classified information must never be processed on an unclassified information system

Classified IS: In case of…

- **Before any hardware or software can be used in conjunction with a classified IS, it must be approved by your ISSM in collaboration with the government**
- **Only authorized personnel are permitted to load or install software or hardware on a classified system**
- **Important information to know when dealing with unexpected computer incidents:**
  - **Don’t touch or delete anything**
  - **Notify ISSM as soon as possible**
  - **When using a classified computer system, if there is an indication of a virus, immediately contact the ISSM**
  - **If you have reason to believe that any suspicious activity has taken place on your system, contact your ISSM immediately**

Classified Information Systems

- **In today's world, much of our classified information is processed on a computer; however, classified information can be compromised in a multitude of ways to include conversations**
- **Classified information that is spoken verbally is harder to regulate than the previously mentioned instances. This is why it is important to practice proven communication safeguards. This practice is known as Communications Security or COMSEC**



Communications Security (COMSEC)

Communications Security (COMSEC)

- **Today, foreign agents, moles and hackers have access to the tools and skills needed to take advantage of any weakness in our COMSEC methods**
- **Our greatest vulnerability lies in regular everyday communication between individuals and/or facilities**

Never discuss classified information over an unsecured phone line

COMSEC: Telephones

- **Classified conversations over the telephone should only be done on Secure Telephone Units (STU III) and Secure Telephone Equipment (STE). They can be both secure and unsecured. Check with your local security representative for their procedures involving the use of these communication lines**
- **When conducting telephone conversations using secured methods, confirm an individual's facility clearance and Need-to-Know before discussing any classified information**

Visit Requests

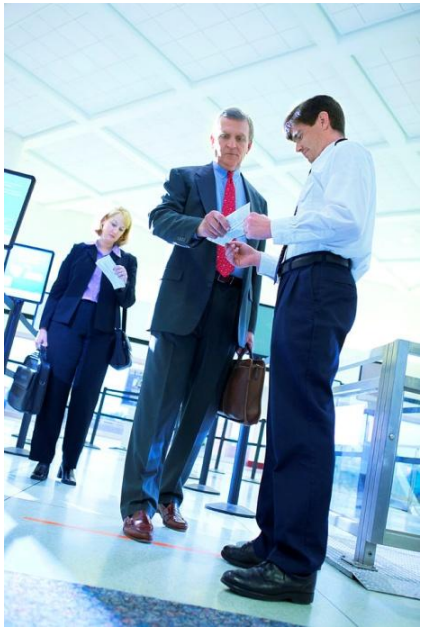
Visit Requests

- **If you are going to another Lockheed Martin facility and accessing classified information, you are not required to process a visit request. However, if you are required to travel on behalf of the company and access classified information at another company or a government customer, you may be required to send a visit request**
- **To send a visit request, contact LMSecurity at 866-330-7311**

If the visit request is unclassified, requires access to SCI or SAP areas or information, or involves travel overseas, see your local security representative for instructions

International Outgoing Visit Requests

- **For classified International Visits to a U.S. Military or U.S. Government Installation ONLY, please contact your local security representative five days in advance of the visit**
- **Classified International Visits to contractor facilities must be submitted on a specific DoD form at least 45 days in advance**



Travel Procedures

Travelling in High Risk Countries

- **Certain countries have been identified by the State Department as being particularly high risk to United States citizens and contractor travelers**
- **The specific list of hostile countries can change frequently. Before you leave the country, please be sure to contact your local security representative to find out updated threat information by country**

Travel Procedures

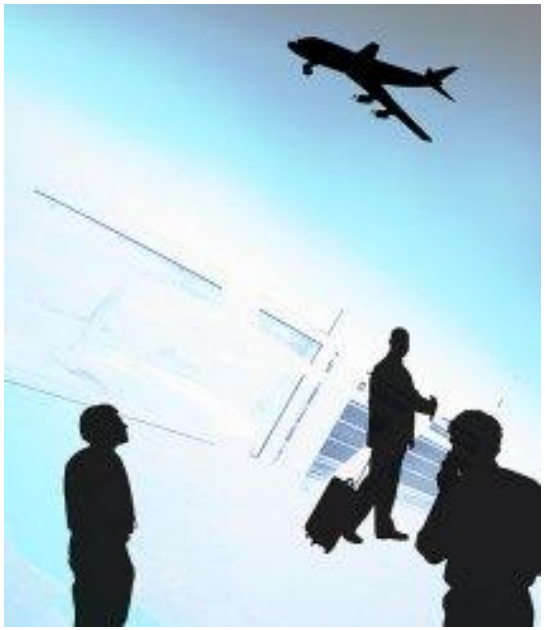
- **Typically, visit requests involve traveling to another location. Because you hold a security clearance, it is now more important than ever to make sure you are following safe (and smart) travel procedures. Lockheed Martin values the safety of our employees. In order to be able to receive assistance if needed or necessary, inform your management of any travel, both business-related and personal**

- **Major travel threats include:**
  - **Criminal threats (robbery)**
  - **Terrorism threats (area visiting changes threat level)**
  - **Hostile, economic or competitive intelligence threats (financial requests, prevent freedom of traveler, etc.)**

- **Suspicious Contacts:**

  Any unusual contact needs to be reported via requiredreports.lmsecurity@lmco.com or to your local security representative

Travel Preparations



When preparing to travel:

- **Do not publicize your travel plans**
- **Make sure that your Passport and Visa are valid, if traveling internationally**
- **Avoid airport disturbances**
- **Never leave luggage unattended**
- **Pay attention to your belongings at the X-ray conveyor belt**
- **Be patient and cooperative with airport officials**
- **Avoid bringing attention to yourself**
- **Practice common sense at all times**
- **Be aware of your surroundings at all times**

LMSecurity

LMSecurity

- **LMSecurity, a corporate-wide initiative, has implemented a new Department of Defense (DoD) industrial security program across the corporation to consolidate the security clearance process. As a part of this initiative, the Orlando-based LMSecurity Operations Center (LMSOC) was expanded into a centralized facility to support DoD clearance processing for the entire corporation**

- **For any security related questions or clearance needs please contact LMSecurity at:**

866-330-7311
407-306-7311
100 Global Innovation Circle
Orlando, FL 32825
Clearances.lmsecurity@lmco.com

Conclusion

Today's training focused on the importance of your personal security responsibilities. It is imperative that we do our part to maintain the trust placed in us by the Department of Defense to protect its most vital secrets

Remember…

- **Report any unusual or suspicious activity**
- **Never forget that our adversaries will go to any lengths to acquire U.S. technology, so take care that DoD classified information is properly safeguarded**
- **Be sure that only those with the Need-to-Know have access to our information**
- **There are Lockheed Martin employees worldwide holding DoD clearances. Never underestimate your importance as the first line of defense in protecting classified information**
- **Remember, you're never alone in this effort. A professional Lockheed Martin security team stands ready to help you. If you don't know the answer to a security question, don't guess. Ask your security representative**