



# DEPARTMENT OF DEFENSE (DoD) INITIAL TRAINING GUIDE

Lockheed Martin Security

# TABLE OF CONTENTS

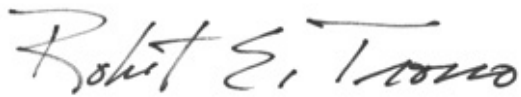
Congratulations	2
Introduction	3
Reporting Requirements	4
Procedures and Duties	5
Safeguarding	6
Reproduction	6
Transmission	6
Retention/Disposition	6
Classification Overview	8
Counterintelligence	9
Conclusion	10
Obtaining Training Credit	10
Glossary	11

# CONGRATULATIONS

You have been granted a Department of Defense (DoD) security clearance and consequently the U.S. government has provided authority for you to access certain classified information.

As a cleared individual, there are basic security concepts you will need to learn. This training guide will provide the foundational knowledge, expectations and requirements you will need to understand prior to beginning work. After 30 days, you will take an online course that will recap much of this information, along with scenario-based exercises that will test your understanding of the material. You will also get to know Security Professionals who can assist and guide you in maintaining a strong, defensive security posture.

Thank you for your attention to this important topic, and welcome aboard!

A handwritten signature in black ink that reads "Robert E. Trono". The signature is fluid and cursive, with the first name "Robert" and last name "Trono" being clearly legible, and "E." in the middle.

Bob Trono  
Vice President & Chief Security Officer  
Lockheed Martin

# INTRODUCTION

## INDIVIDUAL SECURITY RESPONSIBILITIES

The U.S. government has established detailed requirements which are outlined in the National Industrial Security Program Operating Manual, or NISPOM, to ensure the protection of classified information. Part of your role as a cleared Lockheed Martin employee is to protect our nation from a variety of threats. Our National Security is constantly under attack by adversaries both foreign and domestic; by protecting classified information, you are fulfilling a critical role in protecting our nation.

This training guide will provide security procedures that are critical for cleared employees to understand and comply with government security regulations. Although each cleared facility adheres to set government security standards, implementation procedures may vary from site to site.

## PENALTIES

Penalties for unauthorized disclosure of classified information, which can be assessed against both cleared employees and the corporation, include:

- Fines of up to \$10,000
- Imprisonment of up to 10 years



**For defense contractors such as Lockheed Martin, the Defense Security Service (DSS) is the primary DoD security agency assigned to oversee the protection of classified information.**

# REPORTING REQUIREMENTS

Now that you are a cleared employee, there are a number of reporting requirements you must adhere to in order to maintain your security clearance. These reporting requirements are centered on events and activities that could potentially impact your ability to protect classified information.

## CHANGE IN PERSONAL STATUS

- Name
- Citizenship including acquiring dual citizenship and/or foreign passports
- Residence
- Marital status
- Cohabitation in a spouse-like relationship with a foreign national
- Job assignment no longer requiring a security clearance

## SUSPICIOUS CONTACT

- Any contact with an individual that is suspicious in nature, whether they are a U.S. or foreign person
- Someone taking an unusual interest in you and your job and/or asking probing questions about what you do and who you work for

These contacts can occur online, through social media, email, via phone, written correspondence, or in person.

Some examples of suspicious contacts include:

- Request for protected information under the guise of a price quote or purchase request, market survey, or other pretense
- Attempts to entice cleared employees into situations that could lead to blackmail or extortion
- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export license on file
- Attempts to place cleared personnel under obligation through special treatment, favors, gifts, or money

These reports should be made to the local Security Office or to the LMPeople system internally. If in doubt as to whether something is reportable, consult with your Security Office.

## ADVERSE INFORMATION

You must also report information that reflects unfavorably on the integrity or character of yourself or another cleared individual that may impair the ability to safeguard classified materials. This information is defined as adverse information.

Some examples of adverse information include:

- Known or suspected violation of security rules by you or another individual
- Known or suspected compromise of classified information by you or another individual
- Any arrest, criminal activity, or civil court actions
  - Traffic fines over \$300 (not including court fees)
- Treatment for psychological, mental, emotional, and personality disorders and counseling, except family/marriage, grief and combat-related counseling (unless the counseling was precipitated by a violent action or event)
- Substance abuse
- Medical marijuana (prior to use)
- Use of illegal controlled substances (which includes marijuana under federal law)
- Unexplained affluence
- Excessive indebtedness or recurring financial difficulties (e.g., foreclosure or bankruptcy)
- Knowledge of an employee not wanting to perform on classified work
- Close or continuous contact with a foreign person or entity
- Misuse of any company or U.S. government information systems
- Behavior that causes an individual to be vulnerable to coercion, exploitation, or duress and/or reflects lack of discretion or judgement (to include behavior of a sexual nature)

# PROCEDURES AND DUTIES

## LEVELS OF CLASSIFIED INFORMATION

The United States government has three levels of classified information. The level of classification is determined by the degree of negative impact to National Security if improperly disclosed. The classification levels are defined as:

- **CONFIDENTIAL** - This classification is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause **damage** to National Security.
- **SECRET** - This classification is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause **serious damage** to National Security.
- **TOP SECRET** - This classification is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause **exceptionally grave damage** to National Security.

You may sometimes hear classified information referred to as “National Security” information or “collateral” information.



“Collateral” refers to classified materials for which special requirements are not formally established.



Rank, level, or position within the company does not equal a clearance or need-to-know.

## RELEASE OF INFORMATION

Prior to releasing information, the holder must ensure that the recipient of the information has both:

- Proper security clearance – Cleared individuals may access classified information at or below their clearance level
- Need-to-know – Each individual shall only be granted access to the specific classified information that is absolutely required to perform their job.

If you have a question about whether someone should have access to classified materials and information, ALWAYS contact your local Security Office.



# PROCEDURES AND DUTIES (CONT)

## HANDLING OF CLASSIFIED INFORMATION

### Safeguarding

Some general safeguarding guidelines include:

- Never leave classified material unattended
- Secure classified material in a government-approved container or area
- Properly protect combinations that control access to classified materials and areas
- Understand how your facility secures classified materials and areas at the end of each day
- When transmitting classified information outside of a Lockheed Martin facility, comply with all special requirements
- Take actions to prevent the loss or unauthorized disclosure of classified information; be mindful when holding classified discussions (such as hallways, cubicles, break rooms, etc.)
- Be aware of local policies or restrictions regarding cell phones, cameras, MP3 players, tablets, and any other personal electronic device entering classified areas
- Understand the various types of approved areas for classified operations including but not limited to closed and restricted areas
- Recognize that classified material comes in various forms (such as documents, hardware or assets, electronic media, communications or transmissions)



### Reproduction

- Reproduction of classified material:
  - Should always be kept to a minimum
  - Should be performed only by authorized personnel familiar with the procedure
  - Should be performed only on authorized equipment

### Transmission

All classified materials coming in and out of a facility by mail, fax, or courier must be sent and received by the Security Office.

If you receive a classified package directly, notify your local Security Office IMMEDIATELY!

### Retention / Disposition

Contractors are authorized to retain classified material received or generated under a contract for two years following completion of the contract, unless other guidance is provided by the Government Contracting Authority (GCA).

Classified material should only be retained for valid contract performance purposes and dispositioned when no longer needed.

Destruction of classified information must be accomplished by authorized methods and personnel ONLY. Understand the destruction methods at your facility.



**In case of emergency, follow all practical security measures for safeguarding classified material as the situation allows.**

**YOUR PERSONAL SAFETY COMES FIRST!**



# PROCEDURES AND DUTIES (CONT)

## UNAUTHORIZED RELEASE OF CLASSIFIED INFORMATION

There are negative impacts associated with the unauthorized release of classified information. These impacts include but are not limited to:

- Damage to National Security
- Weakened integrity of classified information and technical advantage
- Damage to company reputation and customer relationships
- Potential negative impact on award fees
- Loss of classified contracts and/or exclusion from bidding
- Loss of personal security clearance and/or employment

## DATA SPILLS

Data Spills, also known as data contaminations, are a form of unauthorized release of classified information. Data spills occur when classified information is either intentionally or unintentionally introduced to an unclassified or unaccredited information system. Improper handling of data is at the core of most data spills.

The best way to prevent a data spill is to focus on what you can control:

- Know where to find and how to use security classification guides for your program or project
- Properly handle and appropriately mark classified information
- If you receive or discover classified or potentially classified information on an unclassified information system, immediately contact your local Security Office for guidance. Do not forward, print, save, or delete the suspected information.



## SECURITY INCIDENT REPORTING

The improper safeguarding, handling, reproduction, transmission, disposition, or disclosure of classified material is a reportable security incident.

If you commit or discover a potential security incident, immediately report the circumstances to your local Security Office and, if possible, ensure the material involved is properly safeguarded. When reporting an incident, be cognizant not to disclose classified information over unsecure means.

Security personnel will evaluate the circumstances and take actions as appropriate.

By adhering to security procedures, you ensure that classified information is properly protected and contribute to the nation's security.

By properly protecting information, we meet our contractual obligations, enhance customer trust, help ensure Lockheed Martin's continued ability to compete for new business opportunities, and maintain our reputation as an industry leader.



# CLASSIFICATION OVERVIEW

Information becomes classified by a designated **Original Classification Authority** after it has been determined the information is owned, produced by or for, or controlled by the United States, and that unauthorized disclosure could result in damage to National Security.

When marking classified material (i.e. documents, media, or electronic files), the following must be included:

- The overall level of classification
- Title of the material
- Date created
- Name and address of the originating facility
- Identity of the classifier
- Period of time protection is required
- Any sources used to classify the information
- Any portions that contain classified information

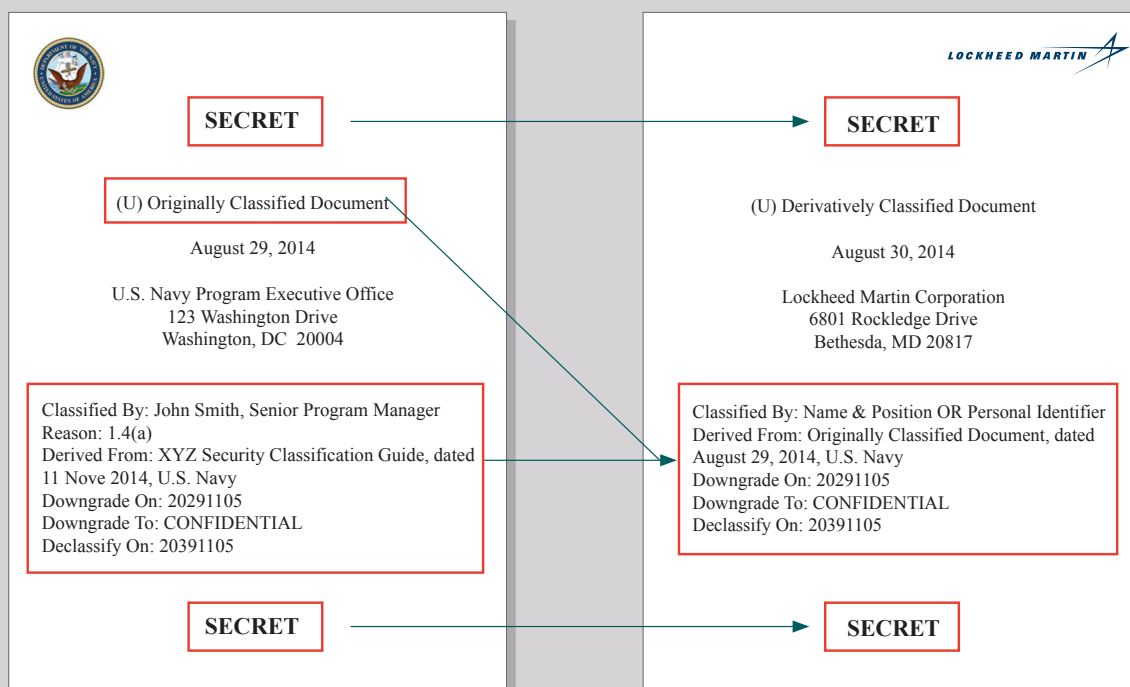
Classification markings may be identified from the following two places:

- Security Classification Guides (SCGs) or equivalent guideline authorized for your effort
- Existing properly marked source material authorized for use on your effort

Classification markings help facilitate proper safeguarding requirements and assist in the prevention of inadvertent release.

You may be required to perform **derivative classification decisions** in the course of your job responsibilities; if this is the case, you will receive additional training in greater detail.

Carrying forward these markings to newly-generated material is our responsibility as contractors, who make derivative classification decisions when we include existing classified information into new forms.



Classification markings and examples in this guide are for training purposes only.

# COUNTERINTELLIGENCE

Counterintelligence is defined as information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage or sabotage; conducted for or on behalf of foreign powers, organizations, international terrorist groups or individuals.

## What does that mean to you?

Counterintelligence is identifying intelligence threats to Lockheed Martin and our government customers, and developing strategies to mitigate those threats.

As a newly cleared employee with Lockheed Martin, it's important you understand these threats.

Intelligence threats can come from foreign intelligence services, foreign and/or domestic industry competitors, criminal, terrorist, and/or extreme activist organizations, and trusted insiders, also known as the insider threat.

Intelligence collection can come in a variety of different forms, including: elicitation, open source collection, electronic surveillance, cyber intrusions, social engineering, exploitation of social media, and formal recruitment.

Recruitment occurs when an employee collects information on behalf or at the direction of a foreign intelligence service. Formal recruitment is often the precursor to insider threat activity.

The insider threat is someone who has legitimate access to company or classified USG information and uses that access to steal information for their

foreign intelligence service, on their behalf. Indicators of insider threat activity might include an apparent disgruntlement with employer or USG, disregard for security and IT procedures, outward expression of loyalties towards competitors or foreign nations, unreported foreign travel or foreign contacts, or a sudden shift in demeanor.

The ultimate goal of a foreign intelligence officer is successful recruitment of an employee who can act as an insider on their behalf. As a Lockheed Martin employee and a member of the cleared community, you are an elevated target for recruitment and intelligence collection by those that seek access to classified information and classified information systems.

You are also in the best position to observe behaviors suggesting concerns of an insider threat in the workplace. Employee should contact their local Security Office immediately if they have concerns they've been involved in a recruitment attempt or other intelligence collection attempts, or if they have any concerns of potential insider threat activity in the workplace.



# CONCLUSION

## **This guide provided you with information on:**

- Your reporting requirements
- The security duties and procedures applicable to your job
- The Security Classification System
- Counterintelligence, the insider threat, and defensive security practices to mitigate these threats

Remember that each facility supports unique contracts and may implement requirements in slightly different ways. To be successful in your new role as a cleared Lockheed Martin employee, it is imperative that you work closely with your local Security Office regarding the content reviewed in this guide and any additional facility specific requirements.

Now that you have received your security clearance, you play an integral part in ensuring the success of the Lockheed Martin Security Program and our National Security. The nature of your new responsibilities relates directly to our customers.

Please continue to the instructions on receiving credit for this course.

## **Completing the Training Acknowledgement form**

Now that you have completed this training, please [click here](#) to retrieve and complete the Training Acknowledgement form. The following options are available to you for submitting this form:

- Fax without a cover sheet to LMSecurity at (720) 479-2750
- Email a digital copy of the requested document to:

**faxserver.lmsecurity@lmco.com**

- Mail the requested document overnight to:

**Lockheed Martin Corporation**

**Attn: LMSecurity**

**100 Global Innovation Circle, MP801**

**Orlando, FL 32825**

**Once LMSecurity receives your form, training credit will be given via our internal training system.**

# GLOSSARY

**Collateral** – All National Security information classified Confidential, Top Secret or Secret under the provisions of an executive order for which special community systems of compartmentation (e.g., non-Special Compartmented Information (non-SCI)) are not formally established

**Confidential** – A level of classification that is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause damage to National Security

**Courier** – An individual who has been briefed and meets the requirements to transport classified materials

**Derivative classification decisions** – The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that applies to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

**DoD** – Department of Defense

**DSS** – Defense Security Service

**GCA** – Government Contracting Authority, which provides guidance to contractors

**Need-to-know** – must be in place along with a security clearance to be granted access to specific classified information required to perform a job

**NISPOM** – National Industrial Security Program Operating Manual

**Secret** – A level of classification that is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause serious damage to National Security

**Security clearance** - An administrative authorization for access to National Security information up to a stated classification level (Top Secret, Secret, Confidential).

*NOTE: A security clearance does not, by itself, allow access to controlled access programs*

**Top Secret** – A level of classification that is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause exceptionally grave damage to National Security

**USG** – United States government



[An extensive list of security terms can be found at the Defense Security Service website.](#)

