



# Department of Defense (DoD) Training Guide

Lockheed Martin Security



# Contents

Congratulations

Introduction

Reporting Requirements

Procedures and Duties

Classification Overview

Counterintelligence

Reducing Vulnerability

Conclusion

Completing the Non-Disclosure Agreement

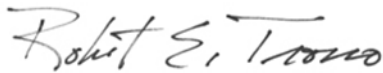
Glossary

# 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 newly 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 "Bob Trono". The signature is written in a cursive, flowing style.

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 Title 32 CFR Part 117 (Formally 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

Criminal penalties for unauthorized disclosure of classified information and trade secrets, which can be assessed against both cleared employees and the corporation, include: financial implications and imprisonment.



*For defense contractors such as Lockheed Martin, the Defense Counterintelligence and Security Agency 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.

## Substance Misuse

Substance Misuse incidents include, but are not limited to:

### Alcohol

- Operating a vehicle under the influence or while intoxicated (e.g. DUI, DWI, BWI, “Wet Reckless”)
  - Note: The term vehicle includes, but is not limited to: automobiles, watercrafts, aircrafts, motorcycles, and bicycles
- Public Intoxication
- Underage consumption of alcohol
- Treatment for alcohol use
- Intoxicated or impaired at work

### Drugs

- Testing positive for an illegal drug
- Use of any illegal drugs or controlled substance
  - Note: Marijuana remains illegal under federal law, regardless of current state laws
- Any substance misuse (to include prescription drugs)
- Failure to complete drug treatment program when prescribed
- Treatment for drug use
- Intoxicated or impaired at work

## Criminal Conduct

Criminal Conduct incidents include, but are not limited to:

- Any arrest regardless of charges being dropped or dismissed
- Domestic Violence
- Warrants or Failure to Appear
- Assault/Battery
- Restraining Order
- Trespassing
- Violation of probation
- Possession of any controlled substance to include marijuana
- Disorderly Conduct
- Any criminal citation, even if an arrest is not involved

## Misuse of Information Technology

Misuse of Information technology includes, but is not limited to:

# Reporting Requirements

- Unauthorized entry into any information technology system
- Unauthorized searching/browsing through classified computer libraries
- Unauthorized modification, destruction, manipulation, or denial of access to information residing on a computer system
- Unauthorized introduction of media into any computer system
- Storing or processing classified information on any system not explicitly approved for classified processing
- Attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator, other than as part of a legitimate system testing or security research
- Downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized system/device or person

## Financial Considerations

There are unique reporting requirements depending on your security clearance level, please see below:

### CONFIDENTIAL/SECRET

Financial Consideration incidents include, but are not limited to:

- Bankruptcy
- Foreclosure or short sale
- Evictions
- Debts to collections
- Charge offs
- Wage garnishments
- Repossessions
- Tax lien or tax levy
- Debt consolidation when involving delinquent debts
- Debts 120+ days delinquent
- Gambling that leads to financial problems
- Delinquent child or spousal support payments

### TOP SECRET

Financial Consideration incidents include, but are not limited to:

- Bankruptcy
- Foreclosure or short sale
- Evictions
- Debts to collections
- Charge offs
- Wage garnishments
- Repossessions
- Tax lien or tax levy
- Debt consolidation when involving delinquent debts
- Debts 120+ days delinquent

# Reporting Requirements

- Gambling that leads to financial problems
- Delinquent child or spousal support payments
- Monetary gains of \$10,000 or greater (inheritance, winnings, or similar financial gain)

## Handling Protected Information

Handling Protected Information incidents include, but are not limited to:

- Loss or compromise of classified information
- Multiple security incidents (such as discussing classified information on non-secure phone, not properly securing classified information or areas, personal electronic devices in secure area)
- Data spill (sending or storing classified information via an unclassified system)
- Storing classified information outside approved facilities and/or containers
- Revealing of classified information to unauthorized persons, including news media
- Inappropriate, unusual, or excessive interest in classified information outside one's need-to-know
- Statements or actions that demonstrate an individual believes the security rules do not apply to him/her
- Pattern of mishandling of unclassified, but otherwise controlled/sensitive, information
- Deliberate disregard for information protection policy or exhibiting negligence to safeguard information

## Psychological and Emotional Health

Lockheed Martin and the U. S. government recognize the critical importance of mental health, and we advocate proactive management of mental health conditions to support the wellness and recovery of all employees. While most individuals with a mental health condition do not present a security risk, there may be times when such a condition can affect a person's eligibility for a security clearance. Mental health treatment, in and of itself, is not a reason to revoke or deny access to classified information.

Note: If not inclusive of one of the below conditions, counseling or treatment related to marital, family, grief, service in a military combat environment, victims of sexual assault and/or domestic violence, depression, anxiety, attention deficit disorder (ADD), attention-deficit/hyperactivity disorder (ADHD) and/or obsessive-compulsive disorder (OCD) are not reportable circumstances. Likewise, in and of itself, voluntarily seeking counseling from medical professionals or independent programs (e. g. Lockheed Martin's Employee Assistance Program [EAP]) is not reportable. Should you have any additional questions or concerns relating to mental health and your security clearance, please contact [requiredreports.lmsecurity@lmco.com](mailto:requiredreports.lmsecurity@lmco.com).

Psychological and emotional health incidents include, but are not limited to:

- Court or administrative agency declaring one mentally incompetent
- Court or administrative agency ordering one to consult with a mental health professional
- Hospitalization for any mental health condition (voluntary or involuntary)

# Reporting Requirements

- Diagnosed with any of the following conditions: psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder, or antisocial disorder
- Pattern of significant change from past behavior
- Failure to follow prescribed treatment plan related to a diagnosed psychological/psychiatric condition, including but not limited to, failure to take prescribed medication or failure to attend required counseling sessions
- Mandated to participate in Employee Assistance Program (EAP)
- Extreme or recurrent statements of bitterness, resentment, vengeance, or disgruntlement that suggest a risk of some illegal or improper action
- Any other behavior that casts doubt on an individual's judgment, stability, reliability, or trustworthiness, not covered under any other guideline that may include: irresponsible, paranoid, manipulative, impulsive, exploitative, or bizarre behaviors

## Personal Conduct

Personal Conduct incidents include, but are not limited to:

- Company policy violations (mischarging, misuse of assets, harassment, misconduct, etc.)
- Threats of violence
- Traffic citations of \$300 or more
- Recurring pattern of poor judgment, irresponsibility, or emotionally unstable behavior
- Deliberate omission or falsification of material information about background when applying for employment or security processing
- Violations of law or rule while in another country (including violation of U.S. law, even if legal in the foreign country)
- Attempted elicitation, exploitation, blackmail, coercion, or enticement
- Pattern of self-destructive or high-risk sexual behavior that the individual is unable to stop
- Any other behavior that casts doubt on an individual's reliability or trustworthiness that may include: Actual or threatened use of force or violence in an effort to change government policy, prevent government personnel from performing their assigned duties, or prevent others from exercising their constitutional rights, known participation in any organization or group advocating or threatening use of force of violence

## Foreign Influence/Foreign Activities

There are unique reporting requirements depending on your security clearance level, please see below:

### CONFIDENTIAL/SECRET

Foreign Influence incidents include, but are not limited to:

- Continuing contact with foreign nationals involving bonds of affection, personal obligation, intimate contact or exchange of personal information. Examples include, but are not limited to:
  - Dating, cohabitating, marriage to a foreign national
  - Exchange of personal information is reportable when all of the following are met:



# Reporting Requirements

- Contact is reoccurring or expected to reoccur
  - Name and nationality are known during or after exchange
  - Information provided is not accessible by the public nor willingly released by the cleared individual
- Changes regarding nature of contact with foreign nationals (interaction ceases, relationship status changes such as dating to cohabitating or marriage, citizenship changes for the foreign national such as renouncing foreign citizenship or obtaining U.S. citizenship)
- Providing aid/support to a foreign person, group, organization, or government in a way inconsistent with the interests of the U.S.
- Vulnerability to pressure or coercion by any foreign interest
- Ownership of foreign state-backed, hosted, or managed cryptocurrency and cryptocurrency wallets hosted by foreign exchanges
- Application for and/or receipt of foreign citizenship (dual citizenship)
- Application for, possession, and/or use of foreign passport or identity card for travel
- Any employment or service, whether compensated or volunteer, with a foreign government, national, organization or other entity
- Contact with a known or suspected foreign intelligence entity

## TOP SECRET

Foreign Influence incidents include, but are not limited to:

- Continuing contact with foreign nationals involving bonds of affection, personal obligation, intimate contact, or exchange of personal information. Examples include, but are not limited to:
  - Dating, cohabitating, marriage to a foreign national
  - Foreign national roommate who co-occupies a residence for a period of more than 30 calendar days. Examples include, but are not limited to:
    - Roommate (a person with whom the cleared individual resides with for reasons of convenience)
    - Live-in childcare providers
    - Foreign exchange student
  - Exchange of personal information is reportable when all of the following are met:
    - Contact is reoccurring or expected to reoccur
    - Name and nationality are known during or after the exchange
    - Information provided is not accessible by the public nor willingly released by the cleared individual
  - Changes regarding nature of contact with foreign nationals (interaction ceases, relationship status changes such as dating to cohabitating or marriage, citizenship changes for the foreign national such as renouncing foreign citizenship or obtaining U.S. citizenship)
- Providing aid/support to a foreign person, group, organization, or government in a way inconsistent with the interests of the U.S.
- Vulnerability to pressure or coercion by any foreign interest
- Ownership of foreign state-backed, hosted, or managed cryptocurrency and cryptocurrency wallets hosted by foreign exchanges

# Reporting Requirements

- Application for and/or receipt of foreign citizenship (dual citizenship)
- Application for, possession, and/or use of foreign passport or identity card for travel
- Direct involvement in foreign business
- Foreign bank accounts
- Ownership of foreign property
- Voting in a foreign election
- Adoption of a non-U.S. citizen child(ren)
- Any employment or service, whether compensated or volunteer, with a foreign government, national, organization or other entity
- Contact with a known or suspected foreign intelligence entity

## **Business or personal foreign travel must be reported prior to your trip start date using Traveler's Suitcase**

Visit MyLM > Security & Travel > Traveler's Suitcase > Travel Reporting > Initiate a New Trip

Note: Reporting international personal and business travel (travel outside of the United States, U.S. possessions and territories) to the U.S. government is a requirement for all personnel who maintain a U.S. government security clearance eligibility. All other provided information is for internal Lockheed Martin use. Foreign travel booked through the Corporate Travel System will automatically create a trip record in Traveler's Suitcase.

Travel reporting should include travel documents (passport, visa, other), transportation segments (including layovers), and lodging (if applicable).

Note: U.S. government security clearance eligibility holders assigned outside of the United States traveling within their country of origin and travel to Puerto Rico, Guam, or other U.S. possessions and territories, are not considered foreign travel and do not need to be reported.

**If you travel using a foreign passport (i.e., non-U.S. issued) you must report such activity prior to departure through the [Security Central Portal](#) > Report Required Information > Foreign Influence/Foreign Activities.**

## **Other Reporting Requirements**

There are unique reporting requirements depending on your security clearance level, please see below:

CONFIDENTIAL/SECRET

Other Reporting Requirements include, but are not limited to:

- Change in personal status

# Reporting Requirements

- Marital status (civil marriages/divorce/widowed and legally recognized civil unions and domestic partnerships)
  - Change of name
- Requests/queries from the media for classified information or other government information specifically prohibited by law from public disclosure. This could include inquiries regarding classified programs other than for official purposes or customary business practices
  - Note: In addition to reporting such requests to the responsible Lockheed Martin Security Office will also inform the applicable Communications office of the reported circumstances
- Participation in or support of acts against the U.S. or placing the welfare or interest of another country above those of the U.S.
- Attempted elicitation, exploitation, blackmail, or enticement to obtain classified or other controlled/sensitive information specifically prohibited by law or policy from disclosure regardless of means
- Any information that adversely reflects on the integrity or character that suggests a cleared individual's ability to safeguard classified information may be impaired, that access to classified information clearly may not be in the interests of national security, or that the individual constitutes an insider threat

## TOP SECRET

Other Reporting Requirements include, but are not limited to:

- Change in personal status
  - Marital status (civil marriages/divorce/widowed and legally recognized civil unions and domestic partnerships)
  - Change of name
- All cohabitants with whom a cleared individual resides and shares bonds of affection, personal obligation or intimate contact as opposed to a person with whom the cleared individual resides with for reasons of convenience (e.g. a roommate)
- Requests/queries from the media for classified information or other government information specifically prohibited by law from public disclosure. This could include inquiries regarding classified programs other than for official purposes or customary business practices
  - Note: In addition to reporting such requests to Security the responsible Lockheed Martin Security Office will also inform the applicable Communications office of the reported circumstances
- Participation in or support of acts against the U.S. or placing the welfare or interest of another country above those of the U.S.
- Attempted elicitation, exploitation, blackmail, or enticement to obtain classified or other controlled/sensitive information specifically prohibited by law or policy from disclosure regardless of means
- Any information that adversely reflects on the integrity or character that suggests a cleared individual's ability to safeguard classified information may be impaired, that access to classified

# Reporting Requirements

information clearly may not be in the interests of national security, or that the individual constitutes an insider threat

# 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.*



# Procedures and Duties

## 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.



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

## 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)



*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

## **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.





# Procedures and Duties

## 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.

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.

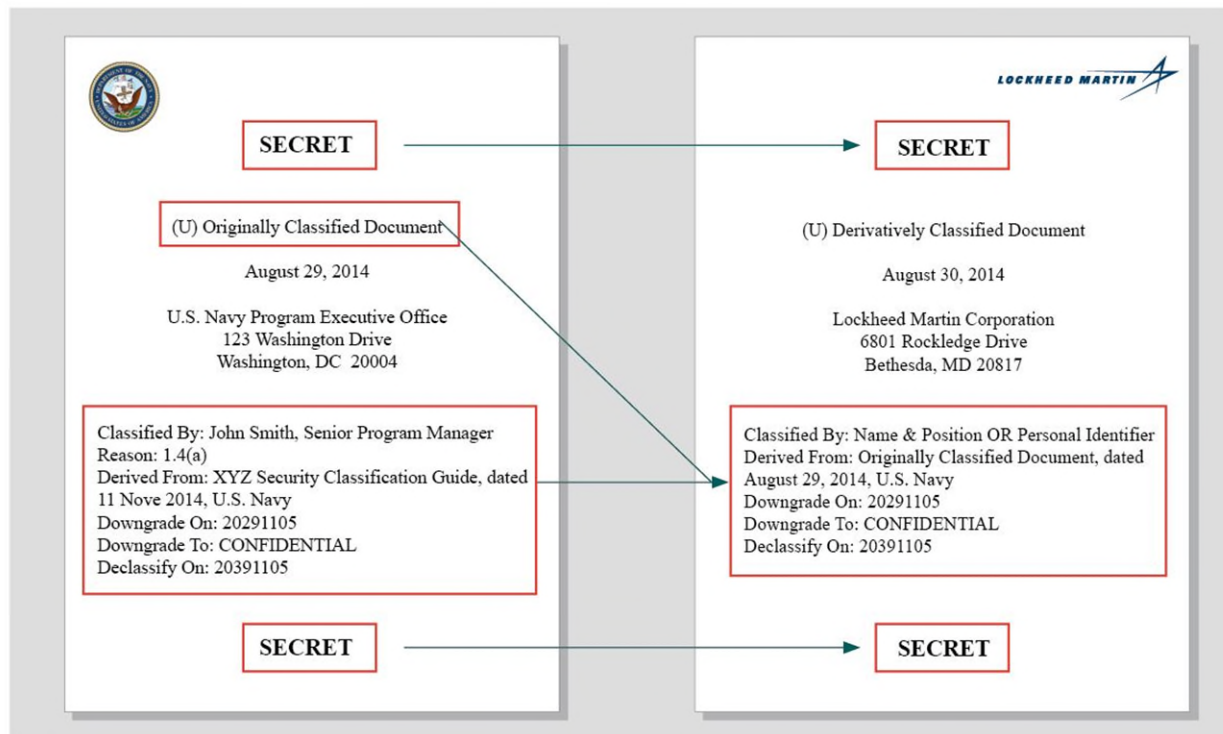


# Procedures and Duties

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 any of the following three places:
- Security Classification Guides
- Source Materials
- Contract Security Classification Specifications or DD Form 254
- 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.

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

# Counterintelligence

Counterintelligence is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage or sabotage; conducted for on or 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 neutralize those threats.

As a newly cleared employee with Lockheed Martin, it's important you're aware of 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.

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.

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

The insider threat is someone who has legitimate access to information and uses that access to steal company or classified USG information for themselves or on behalf of another person or party. Indications 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, etc.

Employees should maintain a keen awareness of their surroundings both in and outside of the workplace and discuss with company security or your customer staff security officer any suspicious incidents or concerns you might have.

			
Foreign Intelligence Services	Foreign and/or Domestic Industry Competitors	Criminal, Terrorist, and/or Extreme Activist Organizations	Trusted Insiders

# Reducing Vulnerability

Employees reduce their vulnerability to these recruitment attempts as well as other attempts at intelligence collection by using social media responsibly, complying with information protection policies, and exercising good judgment while traveling.

- Actions you can take include:
- Utilize privacy and security settings on social media.
- Refrain from mentioning security clearances or sensitive programs on social media posts or profiles.
- Properly follow all company and government classified information system security protocols.
- Refrain from opening links and attachments in unsolicited emails or social media messages.
- Refrain from discussing sensitive or classified information in public or in unapproved areas.
  - This includes discussing sensitive or classified information over unsecured telephones or in any other manner that permits interception by unauthorized persons.
- Reduce your footprint when traveling overseas by using discretion in conversations about your job with unknown persons.

# 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.

# 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

**DCSA** – Defense Counterintelligence and Security Agency

**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

**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 Counterintelligence and Security Agency website.](#)