LOCKHEED MARTIN

Counterintelligence Awareness

Capability Without Compromise

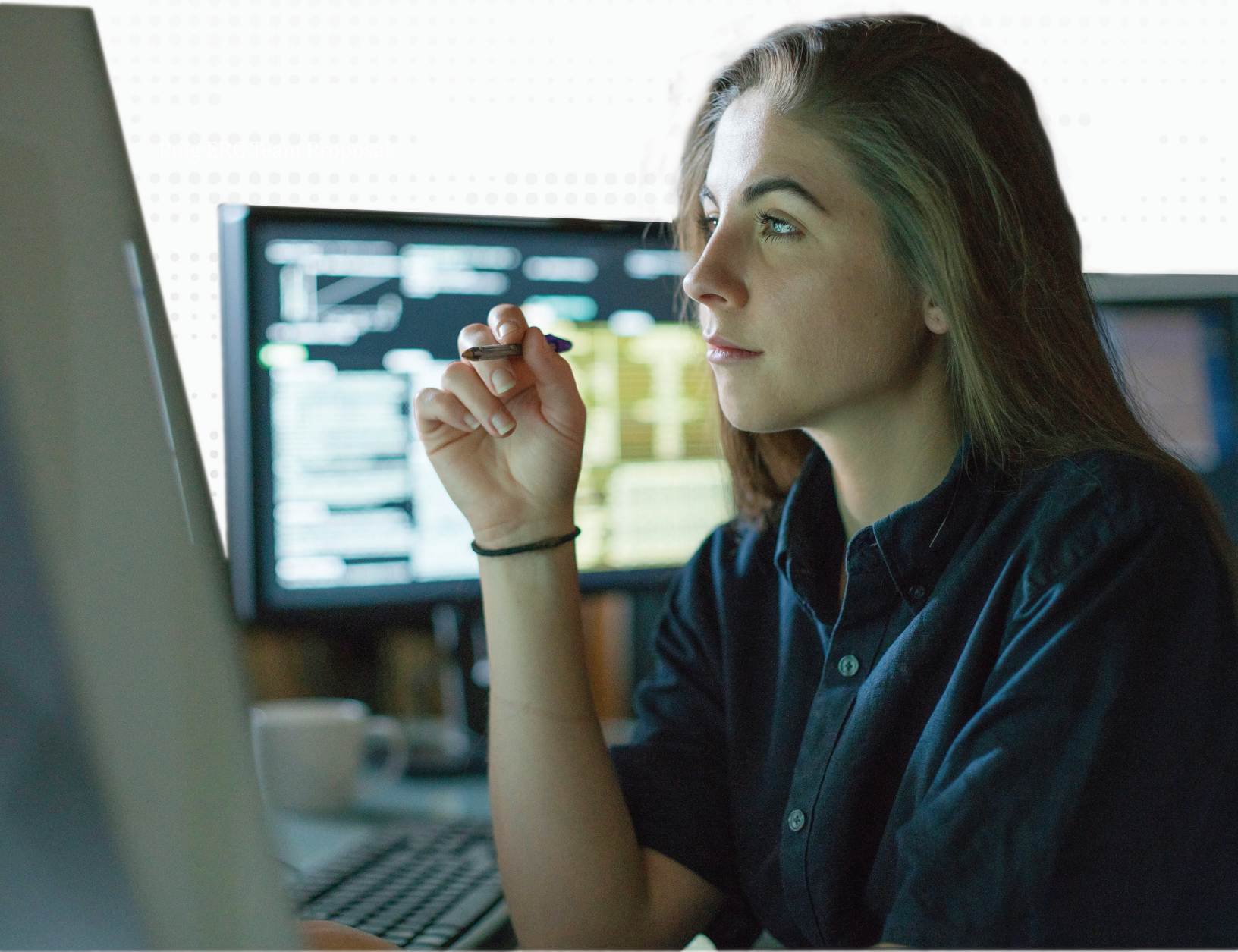


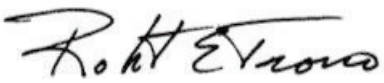
TABLE OF CONTENTS

INTRODUCTION

As a cleared Lockheed Martin employee, you are required to revalidate your security clearance on a yearly basis. Part of this annual clearance review includes completion of a Counterintelligence Awareness Briefing.

Cleared employees are entrusted with a great responsibility in the safeguarding of our U.S. government customers' classified information and a keen understanding of counterintelligence is critical to that responsibility. In this briefing you will review, among other things, targeted information, adversarial methods and tactics, concepts related to the Insider Threat, and employee countermeasures. If you have any questions about the content of this briefing, contact your Facility Security Officer (FSO) for more information.

Thank you for your continued commitment to the role you play in safeguarding our information from threats of espionage.

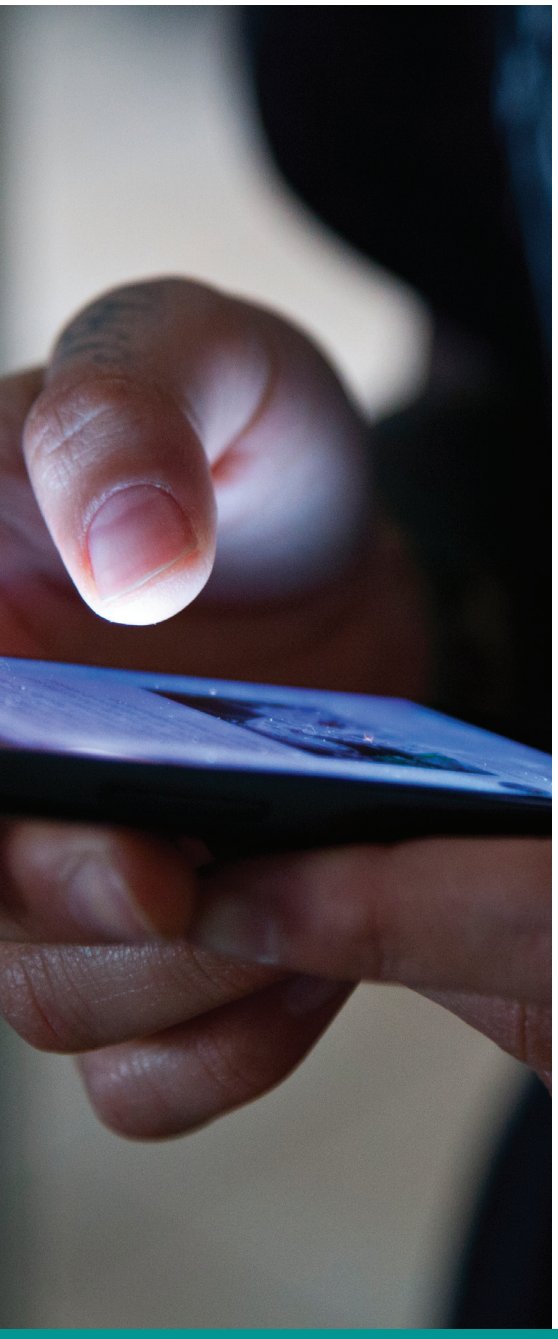


Bob Trono
Vice President & Chief Security Officer
Lockheed Martin

COUNTERINTELLIGENCE DEFINED

According to Executive Order 12333, Counterintelligence (CI) is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

Or simply stated CI is about identifying intelligence threats and developing mitigation strategies to address and neutralize those threats.



THREATS

Intelligence threats can come from many different sources. Here are some examples:

- **Foreign Intelligence Services**

  In 2019, Jerry Chun Sing Lee was sentenced to 19 years in prison after pleading guilty to conspiracy to commit espionage. Lee was a former Central Intelligence Agency (CIA) case officer residing in Hong Kong when he agreed to provide U.S. national defense information to Chinese intelligence officers in exchange for cash.

  Reference: https://www.justice.gov/usao-edva/pr/former-cia-officer-sentenced-conspiracy-commit-espionage

- **Competitors (foreign & domestic)**

  In 2020, Craig German was sentenced to 70 months in prison, a $2,000 fine, and three years supervised release, after pleading guilty to conspiracy to steal trade secrets. German stole aircraft de-icing trade secret documents from the aircraft company for which he worked and then emailed those documents to a competitor company for his own financial gain.

  Reference: https://www.justice.gov/usao-sdga/pr/defendant-who-conspired-steal-aircraft-secrets-sentenced-70-months-federal-prison

- **Insider Threat**

  In 2020, Henry Kyle Frese was sentenced to 30 months in prison for leaking classified information to journalists. Frese was employed by the Defense Intelligence Agency (DIA) as an analyst when he intentionally leaked top-secret information to two journalists; one of whom was his girlfriend. This information ended up published in the public domain.

  Reference: : https://www.justice.gov/usao-edva/pr/former-dia-analyst-sentenced-leaking-classified-information-journalists

- **Terrorist and Extreme Activist Organizations**

- **Criminal Enterprises**

TARGETED INFORMATION

Intelligence collectors will often target a wide array of information in order to piece together a larger picture. While classified information will always be highly coveted by our adversaries, oftentimes corporate proprietary data can be just as desirable. Employees should take care to properly safeguard all of the information they handle, to include:

- Customer data (classified and unclassified)
- Employee data
- Vendor information
- Pricing strategies
- Proprietary formulas and processes
- Technical components and plans
- Corporate strategies
- Corporate financials
- Computer access protocols
- Acquisition strategies
- Marketing strategies
- Investment data
- Business phone and email directories
- Passwords

RECRUITMENT AND COLLECTION TACTICS

Intelligence collectors employ a variety of techniques in their quest to illicitly obtain our information. Some of those techniques include

- Elicitation (collection during seemingly innocent conversation)*
- Coercion or blackmail
- Electronic (i.e. listening devices, cyber intrusions, etc.)
- Collecting information on social media or other open sources
- Recruitment of third parties (i.e. flight attendants, restaurant staff, etc.)
- Exploitation of joint ventures and/or research
- Direct requests for information
- Collection at conventions and air/trade shows
- Hotel room and/or luggage searches
- Inappropriate conduct during facility visits
- Targeting cultural commonalities
- Insider activity

MORE ON ELICITATION

Elicitation is a technique used to discreetly gather information in a way that does not raise suspicion. Conducted by a skilled collector, elicitation may be difficult to detect.

Trained elicitors exploit natural human tendencies or cultural norms, such as the desire to appear well-informed about our profession or a tendency to expand on a topic when given praise.

There are many different elicitation techniques, such as utilizing flattery or criticism, deliberately stating false facts or use of leading questions.

You should politely deflect possible elicitations by:

- Referring person to public sources
- Responding with, “Why do you ask?”
- Giving a nondescript answer
- Simply stating that you do not know
- Advise that you cannot discuss the matter

INSIDER THREAT

The Insider Threat is, current or former employees, contractors, or business partners, with authorized access to company information who misuse that information for their own benefit or that of a competitor or foreign nation

Possible motivations can include greed or financial need, revenge, ideology, divided loyalties, ego, vulnerability to coercion, etc. Some behaviors which might indicate insider activity include:

- Seeks to expand access beyond job requirements
- Sudden reversal of financial situation
- Outward disgruntlement towards employer
- Paranoia that they are under investigation
- Works odd hours inconsistent with job assignment
- Unreported foreign contacts or foreign travel (when required)
- History of security infractions or indifference to policies

EMPLOYEE COUNTERMEASURES

Employees are the first line of defense in safeguarding Lockheed Martin Proprietary and U.S. government classified information. Some simple ways to lower your risk of recruitment and better fulfill your responsibilities as a cleared employee include:

- Maintain a responsible and professional social networking footprint.
- Refrain from identifying yourself as a cleared employee on social or professional networking sites.
- Always utilize encryption when sending sensitive email communications.
- Never release company information beyond what's publicly available.
- Adhere to all company and customer IT policies and procedures.
- Never discuss sensitive information in public places (i.e. restaurants, public transportation, trade shows, etc.).
- Don't respond to questionable electronic communications.
- Maintain a keen awareness of surroundings; notify security of any anomalies or concerns.

FOREIGN TRAVEL CONSIDERATIONS

International travel is advantageous for business and often enjoyed by employees. However, it is important to remember that travel abroad often increases many of the risks we've already discussed. Some mitigation measures to those risks include:

- Travel with loaner electronic devices.
- Use extra caution at airport security lines where theft of electronics devices is rampant.
- Keep a low profile; avoid advertising employee status.
- Refrain from using hotel business centers to log into company networks, and do not use hotel fax, printer, or shredder for sensitive data.
- Disable Wi-Fi and avoid public Wi-Fi networks wherever possible.
- Do not connect foreign storage devices to phone or computer.
- Never leave sensitive data unattended; hotel safes are not secure.
- Understand you have NO expectation of privacy while abroad!

REPORTING TO SECURITY

Timely and accurate reporting from cleared industry is critical in identifying and mitigating collection efforts aimed at our technologies, people and processes. Employees should inform their Facility Security Officer (FSO) immediately upon observation of any suspicious activities, contacts, or behaviors. Some examples include:

- Indications of hotel room and/or luggage searches or intrusions
- Instances of forced surrender of electronic devices during travel
- Suspicious or probing questioning (in person, via telephone, etc.)
- Contact with a known or suspected intelligence officer
- Actual or attempted unauthorized access into LM IT assets
- Direct requests for information
- Abnormal occurrences on electronic devices (i.e. sluggishness, unusual updates, pop-ups, etc.)
- Any unsolicited post-travel contact via email, social media, etc.
- Anomalous or suspicious behaviors in your workplace
- Phishing or attempts at social engineering

Lockheed Martin
6801 Rockledge Drive
Bethesda, MD 20817
www.lockheedmartin.com