Department of Defense

# DIRECTIVE

**NUMBER** 5240.06
May 17, 2011

USD(I)

SUBJECT: Counterintelligence Awareness and Reporting (CIAR)

References: See Enclosure 1

1. PURPOSE. This Directive:

a. Reissues DoD Instruction (DoDI) 5240.6 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (b)).

b. Establishes policy, assigns responsibilities, and provides procedures for CIAR in accordance with DoDD O-5240.02 (Reference (c)).

c. Lists reportable contacts, activities, indicators, and behaviors associated with foreign intelligence entities (FIEs), a term that includes international terrorists.

d. Establishes that persons subject to chapter 47 of title 10, United States Code, hereinafter referred to as the Uniform Code of Military Justice (UCMJ) (Reference (d)) who violate specific provisions of this issuance may be subject to punitive action under Article 92, UCMJ.

e. Establishes that civilian employees under their respective jurisdictions who violate specific provisions of this issuance may be subject to appropriate disciplinary action under regulations governing civilian employees.

f. Includes reportable FIE-associated cyberspace contacts, activities, indicators, and behaviors.

g. Establishes the CIAR Council (CIARC) in accordance with DoDI 5105.18 (Reference (e)).

2. APPLICABILITY. This Directive applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other

# Counterintelligence Awareness and Reporting (CIAR) DoD 5240.06

**Presented By:**
**Michael J. Degnan, SA**
**Hanover Field Office**
**Mid-Atlantic Region**


- Mission & Vision
- Define Counterintelligence (CI)
- You are the Target
- Protecting U.S. Technologies
- MCMO
- Counterintelligence Awareness
- What To Do If Approached
- Potential Espionage Indicators
- Identifying Suspicious Contacts
- Reporting Procedures


**DCSA:** We are our Nation's gatekeepers. We provide Counterintelligence (CI) Functional Services for our cleared Defense Industrial Base (DIB) critical assets and technology through vetting Industrial Security engagement, CI Support to the DoD components, and education IAW DoDD 5240.06. We secure the trustworthiness of the United States Government's workforce, the integrity of its cleared contractor support, the uncompromised nature of its technologies, services and supply chains.

**CI:** Educates, integrates, collects, develops, refers, and disseminates intelligence information to DCSA HQ in order to detect, identify, assess, disrupt or neutralize the foreign threat.

**Guardians of our Nation's assets** - ensuring trust, countering threats and vulnerabilities, and advancing delivery of uncompromised technology.

# What is Counterintelligence?


*Executive Order 12333 was signed by President Ronald Reagan on December 4, 1981*

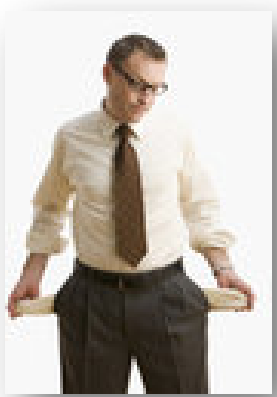
- Information gathered and activities conducted to Identify, Deceive, Exploit, Disrupt, or Protect against Espionage, other Intelligence Activities, Sabotage, and Assassinations conduct for or on behalf of foreign powers, organizations or persons or their agents or international terrorist organizations or activities. -E.O. 12333.
- An activity aimed at protecting an agency's intelligence program from an opposition's intelligence service. It includes gathering information and conducting activities to prevent espionage, sabotage, assassinations or other intelligence activities conducted by, for, or on behalf of foreign powers, organizations or persons.
- Cyber counterintelligence (CCI) is officially defined as: “Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.”
- Counterintelligence adversaries include:
  - Foreign powers
  - Foreign governmental and commercial organizations
  - Foreign persons or their agents
  - International terrorist organizations

# YOU ARE A TARGET


**External** (Cyber Actors, FIE)

- Cyber Operations
- Targeting U.S. Travelers Overseas
- Request for Information (RFI)
- Attempted Acquisition of Technology
- Academic Solicitation
- Seeking Employment
- Exploitation of Relationships
- Solicitation or Marketing Services
- Joint Venture or Business Development

**Internal**
(Employee, Intern, Visitor)
Insider Threat



- Volunteers
- Sleeper Agents
- Co-opted Individuals

# YOU ARE A TARGET


- You possess or have access to classified information and/or information pertaining to technologies that are highly sought after by foreign entities

- Foreign entities will also target information relating to your facility's personnel, security, and operations.

- Remember: Family, Friends, and ***Co-workers*** may be viewed as a means to gain information about you. Always Report Suspicious Behavior or contacts.

- Common sense and basic CI awareness can protect you against Foreign Intelligence Entities attempting to collect classified, sensitive or unclassified information.

Friendly information

Research, development, testing, and evaluation

Program milestones & specifications

System capabilities

**YOU are the first line of defense in protecting classified information and defense technologies!**

# Protect U.S. Technologies


*Technology examples:

Sheyang J-31 F-35

Chengdu J-20 F-22 Raptor

Chengdu J-10 F-16

Caihong-4 MQ-9 Reaper

# Jason Needham

**Crime**: Intentionally accessing a computer network without authorization
**Court**: US District Court
**State**: TN
**Result**: Pled Guilty
**Sentence**: 18 months
**Fine**: $172,394
**Year of Conviction**: 2017
**Age at conviction**: 45
**Employee Type**: Industry Employee
Military: n/a
Job: Engineer
Country of Concern: n/a
**Targeted Technology**: Other

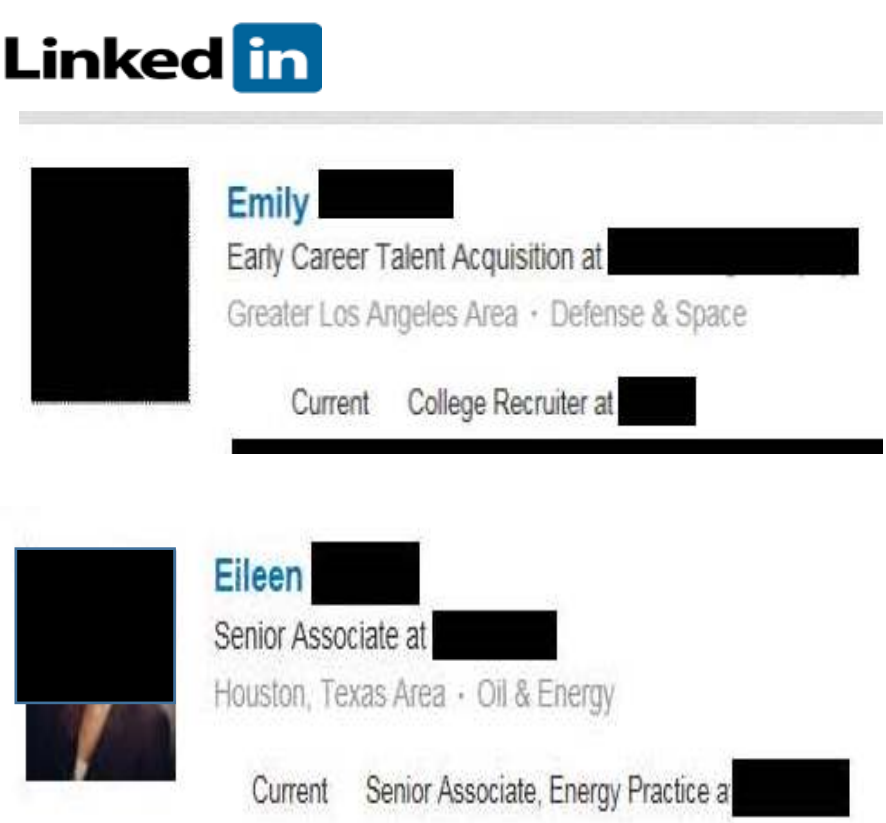
**Indicators: Access Attributes, Financial Considerations, Security and Compliance Incidents**

# Nationwide: Methods of Contact and Methods of Operation (MCMO) Reporting Volume Matrix

Volume of Reporting MCMO Matrix: IBTL CAT W (Command, Control, Communications & Computers (C4))

| METHOD OF OPERATION | METHOD OF CONTACT | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **VOLUME OF INDUSTRY REPORTING** **Blank**= Reporting Gaps | Conference, Conventions or Trade Shows | | Cyber Operations | | Email Request | | Foreign Visit | | Mail | | Personal Contact | | Phishing Operations | | Resume - Academic | | Resume - Professional | | Social or Professional Networking | | Telephone | | Web Form Submission | |
| | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE | Industry | CAGE |
| Attempted Acquisition of Technology | | | | | 5 | | | | | | | | | | | | 1 | | | | | | | |
| Exploitation of Commercial/ Business Activities | | | | | | | 1 | | | | | | | | | | | | 3 | | | | | |
| Exploitation of Cyber Operations | | | 1 | | 1 | | | | | | | | | | | | | | | | | | | |
| Exploitation of Experts | | | | | 2 | | | | | | | | | | | | | | | | | | | |
| Exploitation of Insider Access | | | | | | | | | | | 2 | | | | | | | | | | | | | |
| Exploitation of Relationships | | | | | 1 | | 1 | | | | 1 | | | | | | | | | | | | | |
| Exploitation of Security Protocols | | | | | | | | | | | | | | | | | | | | | | | | |
| Exploitation of Supply Chain | | | | | | | | | | | | | | | | | | | | | | | | |
| Resume Submission | | | | | 6 | | | | | | | | | | 15 | | 53 | | | | | | | |
| RFI/Solicitation | | | | | 3 | | | | | | | | | | | | | | | | | | | |
| Search/Seizure | | | | | | | | | | | | | | | | | | | | | | | | |
| Surveillance | | | | | | | | | | | | | | | | | | | | | | | | |
| Theft | | | | | | | | | | | | | | | | | | | | | | | | |


- Social media is a growing area of vulnerability for individuals and cleared industry
- Social Networking Services (SNS) provide a new tool for foreign intelligence services to collect information on individuals, their work, and their families
- SNS are also vectors for hackers to load malicious content
  - Nearly half the “millennial” generation use SNS while at work
  - Hackers can use message applications or wall postings to create malicious links within the social networking sites
- Other criminals, including identity thieves, use SNS to gain information on likely targets





- Foreign actors increasingly use computer network exploitation to obtain information relating to U.S. technologies
- Methods of exploitation
  - Emails with malicious links or attachments
  - Spoofing email addresses
  - Network software and website vulnerabilities
  - Removable media
- Practical countermeasures

## 1. Moonlight Maze

In 1999, Newsweek revealed the first case of coordinated cyber espionage in the United States. A series of cyber attacks began in 1998 and resulted in thousands of stolen documents containing confidential information about American military technologies. Hackers broke into the network of Wright Patterson Air Force Base and then connected to military research institutions. The Russia was blamed in these attacks, but there was a lack of proves. The malware implemented during the Moonlight Maze operation is still widely used for modern attacks.

## 2. Titan Rain

Within two years from 2003 to 2005, the U.S. government computers were under constant threat arranged by Chinese military hackers. Titan Rain also included attacks on the UK defense and foreign ministries that continued till 2007. This was the first case of cyber espionage sponsored by a state. The hackers penetrated into the network computers using different methods and tried to steal away as much information as possible. The complicity of the Chinese government in this operation wasn't proven, but countries became more cautious about cyber espionage attacks.


## 3. Gillette Industrial Espionage

In 1997, Gillette suffered from industrial espionage after its engineer disclosed corporate information to the company's competitors. Steven Louis Davis worked on the development of a new razor, but then because of quarrels with his supervisor, the engineer stole the designed technology of the new shaver system and revealed it via email and fax to Gillette's competitors. Davis was found guilty in industrial espionage and sentenced to 27 months in jail.

## 4. Office of Personnel Management Data Breach

Starting from 2012, Chinese government hackers allegedly attacked the U.S. Office of Personnel Management and stole personal information about 21 million Americans. As the result of this cyber espionage, perpetrators gained an access to the sensitive data about people who worked or applied for the federal government, including military service. The data leakage was discovered in June 2015 when OPM personnel detected a malware that built a backdoor into the network. A Chinese national suspected in the malware development was arrested only in 2017. Though OPM representatives assured that no one suffered because of hacker's intrusion, the long-term results of this data breach are still unknown.


## 5. Operation Aurora

In the beginning of 2010, Google claimed that the company was attacked by of a series of cyber threats originated from China. Apart from Google, hackers also attacked more than 20 international companies, including Adobe Systems and Yahoo. Google said that its intellectual property was stolen and Gmail accounts were also under persistent threats. The company even considered stopping censoring its search results in China. Attacks were performed exploiting a vulnerability in Internet Explorer and combining stealth programming and encryption techniques.

## 6. GhostNet

In 2009, Canadian researchers revealed a large spy network called GhostNet that arranged an intrusion into more than one thousand computers in 103 countries. Perpetrators got unauthorized access to the network of the Dalai Lama offices and used it for compromising other computers. Besides, the attacks were also performed on the foreign ministers and embassies of Germany, Pakistan, India, Iran, South Korea, and Thailand. The Chinese government denied any involvement in the attacks.

## 7. Night Dragon

In 2011, McAfee reported about the Night Dragon operation initiated by Chinese hackers for attacking the largest European and American energy businesses, including Royal Dutch Shell and Baker Hughes. This was one of the biggest cyber espionage cases when intruders got an access to topographical maps with potential oil reserves. According to McAfee report, attackers used a range of unsophisticated hacking tools and techniques that were available on Chinese hacker websites.


## 8. Spying on the Obama and McCain Computers

Another case of cyber espionage infected the computers of John McCain and Barack Obama during their presidential campaigns in 2008. Chinese or Russian hackers allegedly installed spyware on the computers of these two presidential candidates and stole sensitive data related to foreign policy. The cyber attack was initially considered as a computer virus, but then technology experts discovered a leakage of the considerable amount of files. The data leakage was revealed only after the presidential election during the federal investigation.

## 9. Computer Spies Breach Fighter-Jet Project

In 2009, Pentagon reported that the Fighter-Jet Project came under assault from unknown intruders. This multi-billion project of the next generation fighter became a victim of coordinated cyber espionage attacks during two years. Attackers used computers located in China for stealing a massive volume of data about electronics and internal maintenance. Fortunately, the most sensitive information was kept offline and terrorists weren't able to access it. Though, the U.S. officials suspected Chinese hackers, the true origin of the perpetrators remained undefined.

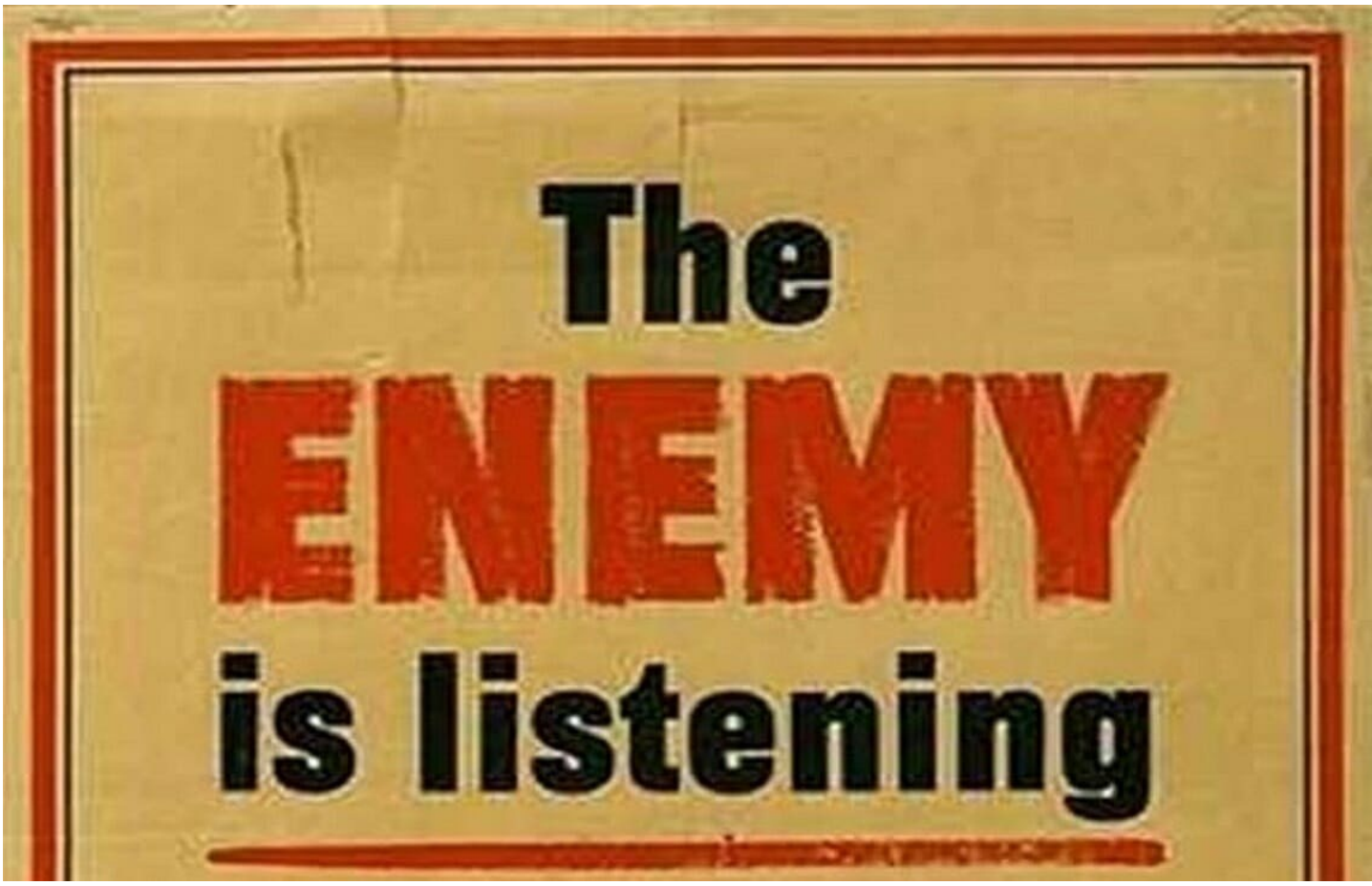

## 10. Operation Shady RAT

Operation Shady RAT is undeniably one of the biggest cyber espionage cases in the history, as it affected more than 70 companies and organizations in since 2006. Victims included the International Olympic Committee that was compromised during several months prior to the 2008 Olympic Games in Beijing. The United Nation and the World Anti-Doping Agency were also under the attack. McAfee identified previously unknown malware that was spread via e-mail with a link to a self-loading remote-access tool, or rat. Cyber terrorists got an authorized access to legal contracts, government secrets, and other sensitive data. Chinese hackers have allegedly arranged the operation, as all countries of Southeast Asia suffered from the attacks except China.

As you can see, cyber hackers can attack you either inside or outside the company, so you should always be ahead of the game. In order to protect your sensitive information against any unauthorized access, consider options for cyber espionage prevention that will ensure employee monitoring and external intrusion blocking.

# Conferences, Conventions, and Trade Shows

- Conferences, conventions, and trade shows present collectors with a target-rich environment due to the abundance of technology, engineers, and technical personnel in attendance
- Collection techniques
  - Elicitation of classified or export-restricted information from subject matter experts
  - Theft of technology on display
  - Photography
  - Collection of business cards and other personal information
  - Gaining access to personal or business electronic devices left unattended
- Practical countermeasures



# Potential Espionage Indicators

- Historically, espionage and terrorism subjects exhibit one or more of the following indicators:
  - Foreign contacts (unreported or attempts to conceal)
  - Foreign preferences/allegiance
  - Security violations
  - Financial concerns
  - Polygraph results (inconclusive or indicate deception)
  - Employment behaviors
  - Personal conduct
  - Foreign travel

Key: Identification of potential espionage indicators involves recognizing a pattern of suspicious activity

# IDENTIFYING SUSPICIOUS CONTACTS


- Examples of suspicious contacts
  - Requests for protected information under the guise of a price quote or purchase request, market survey, or other pretense
  - Foreign entities targeting cleared employees traveling overseas via airport screening or hotel room incursions
  - 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 licenses on file
  - Attempts to place cleared personnel under obligation through special treatment, favors, gifts, or money

# What Do I Do Now

## What To Do If Approached

- If you feel you are being solicited for information:
  - Practice authorized responses to questions concerning your duties
  - Never feel obligated to answer questions which make you feel uncomfortable
  - Change the topic of any conversation that might be too probing with respect to your duties, private life, and coworkers
  - Be observant:
    - Try to note as much as possible about the person asking questions
  - Maintain professional composure

# Report

- **Report, Report, Report**:
  - Provide as much information as possible to your Facility Security Officer (FSO) about the encounter and the individual(s) involved

**DoD 5240.06; section 3, the contacts, activities, indicators, and behaviors in section 5.**

**Employee Identifies and Reports Suspicious Incident**

**FSO**

**Suspicious Contact Report (SCR)**

Local CI Rep

Initial Evaluation/Screening
With follow-up to fully identify the elements of the SCR


**Referrals**

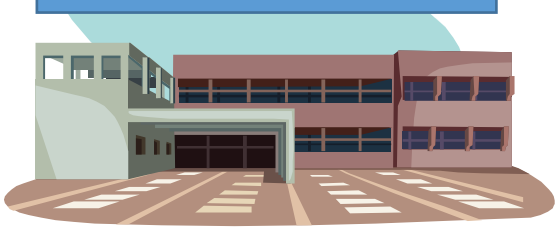
**FBI**

**Local /Federal Counterintelligence and Law Enforcement Agencies**

**SCR**

**DCSA Intel Division (HQ)**

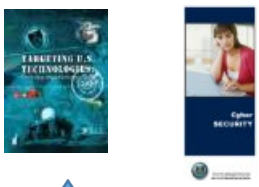
**Local CI/IS Rep**



**Threat Based CI/Security Services**

SCR analytical feedback

**Tailored Threat Products**



**FSO**
Evaluate Products
Adjust CI Program
Employee Feedback
Refine Briefings