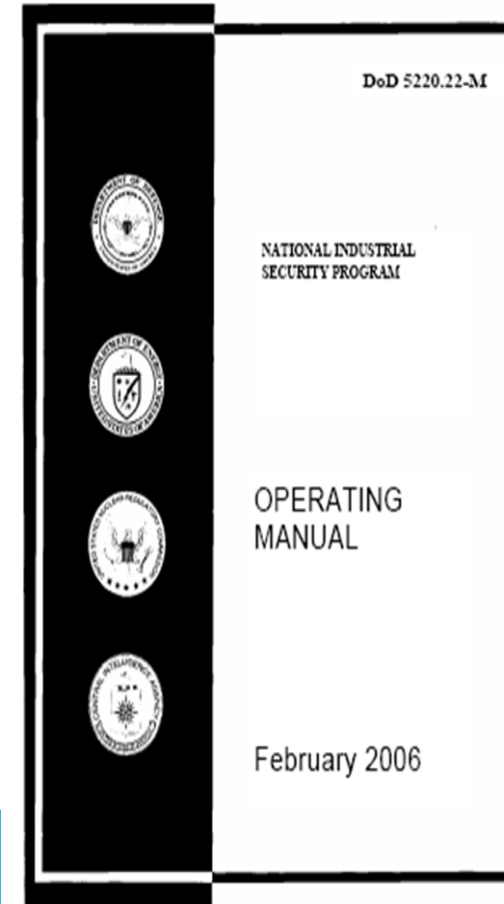


ANNUAL REFRESHER BRIEFING 2018

INTRODUCTION


- Concord Crossroads, LLC is a cleared company in the National Industrial Security Program (NISP)
- Employees are bound by the Department of Defense (DoD) rules and regulations to properly protect and control all classified material in their possession per the National Industrial Security Program Operating Manual (NISPOM) and as appropriate, other cognizant security activities.



INSIDER THREAT

As defined by the Defense Security Service:

Acts of commission or omission by an insider who intentionally or unintentionally compromises or potentially compromises DoD's ability to accomplish its mission. These acts include but are not limited to, espionage, unauthorized disclosure of information and any other activity resulting in the loss or degradation of departmental resources or capabilities.



INSIDER THREAT

Personal Factors

Motives or Personal situations may increase the likelihood someone will spy against their company:

Greed or Financial Need: A belief that money can fix anything. Excessive debt

Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization

Divided Loyalty: Allegiance to another person or company, or to a country besides the U.S.

Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Compulsive and destructive behavior: Drug or alcohol abuse, or other addictive behaviors

Family problems: Marital conflicts or separation from loved ones



INSIDER THREAT CONT....

Organizational Factors

- Some factors on the company's end may make it easier for thieves.
- Classified information is not labeled as such, or is incorrectly labeled
- Undefined policies regarding working from home on projects of a sensitive or proprietary nature
- Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials
- Employees are not trained on how to properly protect proprietary information

Behavioral Indicators

- Interest in matters outside the scope of their duties, i.e. those of interest to foreign entities or business competitors
- Making copies of material, especially if it is proprietary or classified
- Works odd hours without authorization
- Unreported foreign contacts or unreported overseas travel
- Short trips to foreign countries for unexplained or strange reasons

RECENT CASES OF INSIDER THREAT

Reality Winner:

- Former NSA contractor charged with leaking classified documents to a Media Outlet
- Accused of printing out and sending TS documents to the Media Outlet
- Frequently posted and liked various hacking/leaking pages on Social Media
- Documents contained information in reference to the 2016 election and Russian Attempts at Cyber Attacks
- On twitter she was following WikiLeaks, Edward Snowden and several other “ALT” government agency accounts
- Winner “admitted intentionally identifying and printing the classified intelligence reporting at issue despite not having a ‘need to know,’ and with knowledge that the intelligence report was classified
- She pleaded Not Guilty in Federal court
- Recently sentenced to 63 months in prison

Harold Thomas Martin III

- Former NSA employee charged with over 20 counts of theft of classified information
- Accused of stealing over a half billion TS documents over from 1996-2016
- Documents found in his home and car were from NSA, CIA, U.S. Cyber Command, and the National Reconnaissance Office
- All 20 counts are for willful retention of national defense information.
- Each charge carries a maximum 10 year sentence

His attorneys have argued that he didn't share the information with anyone and was simply a compulsive hoarder



COUNTERINTELLIGENCE AND THREAT

- Suspicious Cyber Behaviors and Activities
- Use of account credentials by unauthorized parties
- Tampering with or introducing unauthorized elements into information systems
- Downloading or installing non-approved computer applications
- Unexplained user accounts
- Actual or attempted unauthorized access into automated information systems or networks.
- Multiple agencies conduct counterintelligence activities and produce threat awareness information
- They identify and thwart the adversary's intent to harm U.S. and our allies' interests

Industry is a key component because we:

- Brief employees periodically and attend customer briefings
- Comply with directives, policies and security specifications [DD 254]
- Practice Operations Security [OPSEC]
- Support a thorough reporting program
- Safeguard sensitive and classified information
- Never underestimate the adversary's intentions and capabilities!

Remember:

Mass storage devices are inexpensive and capable of large amounts of data storage;

SUSPICIOUS CONTACTS



What are considered suspicious contacts?

-efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee;
-contacts by cleared employees with knowledge of suspected intelligence officers from any country;
-or any contact which suggests a cleared employee may be the target of an attempted exploitation by the intelligence services of another country

CLASSIFIED INFORMATION

Classified documents are boldly marked with the highest classification on the top and bottom of each page.

Individual Paragraphs have markings: (U), (C), (S), (TS).

Use the Program Security Classification Guide or the contract DD254 for help when marking classified for your contract. These documents will instruct you on what types of information should be classified at which levels.

A 'SECRET' cover sheet form with a red border. The word 'SECRET' is at the top in red. Below it, in small text, is 'THIS IS A COVER SHEET' and 'RESPONSIBILITY OF PERSONS HANDLING THE ATTACHED DOCUMENT(S)'. There are three numbered instructions: 1. Exercise the necessary safeguards to prevent unauthorized disclosure by never leaving classified documents unattended except when properly secured in a safe with approved combination lock. 2. Follow all security regulations applicable to this document, including those regarding registration with Document Control, marking, reproduction, copy numbering, transmission and storage. 3. Individuals who have read or had access to the contents of this document shall affix their signature and date below. (Separate entry for each date.) Below the instructions is a table with four columns: NAME, DATE, NAME, DATE. There are ten rows for signatures. At the bottom, it says 'DO NOT REMOVE THIS COVER SHEET FROM DOCUMENT' and 'This cover sheet is unclassified when separated from classified documents'. Below that is a line for 'Document Control No.' and the word 'SECRET' in red at the very bottom.

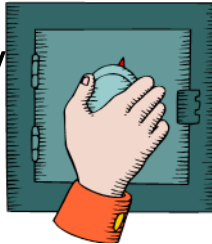
WHEN WORKING WITH CLASSIFIED INFORMATION.....

...close the door! Also, place a sign on the door stating that sensitive processing is going on and to knock before entry. This will give you enough time to secure the material before the person enters.



...close the blinds! If you are in a room with a window, make sure the blinds are closed so that prying eyes cannot peek in and view the material.

...keep it with you at all times! If you must leave the classified, either leave it with a person cleared to the level of the information that has a need-to-know, or give it back to security to lock up for you in its designated GSA approved safe.



...return all classified to its container when you are finished! You may not retain the material overnight.

IS YOUR PHONE TOO SMART?

Vacation Pics posted in Real time....

House Robbed that evening!



Don't tell cause it's a secret...

Not Anymore!

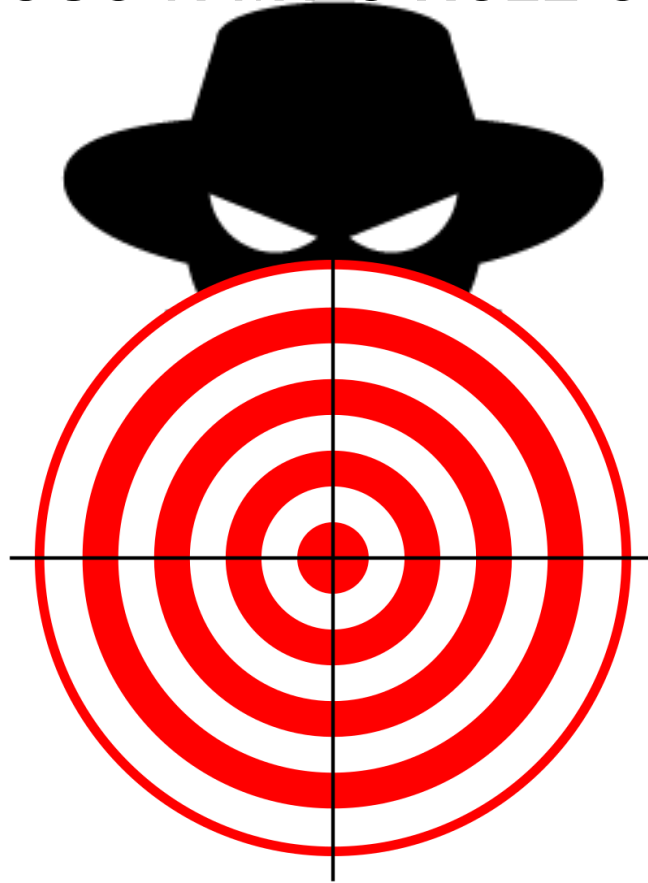


Cell Phone not removed before entering SCIF.....

Hijacked phone as remote listening device!



WON'T YOU JOIN MY CIRCLE OF FRIENDS?

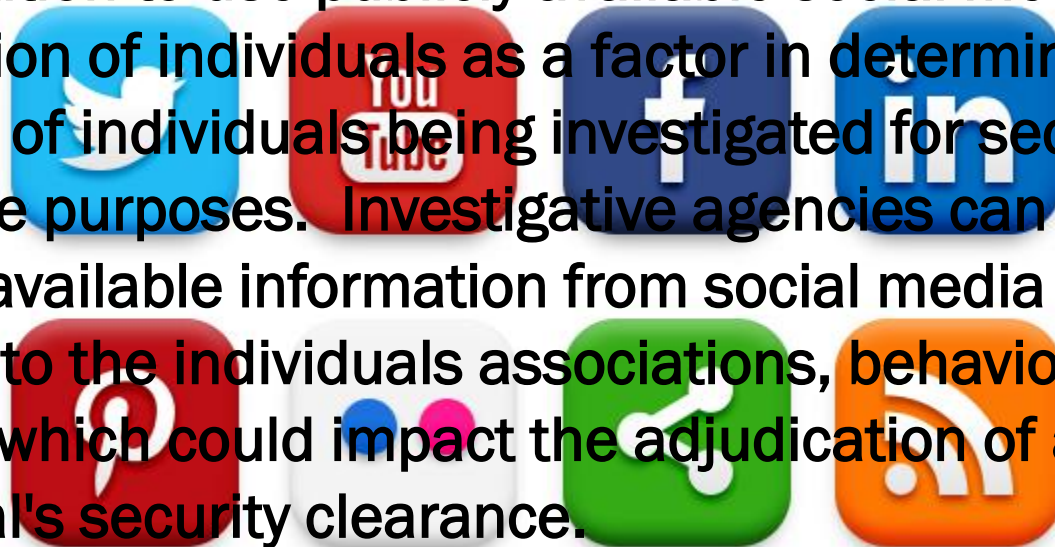


Don't be a target for spies, criminals or terrorists! Use extreme caution online and on social media networks!



SOCIAL MEDIA AND YOUR CLEARANCE

On May 12, 2016, the Director of National Intelligence signed a new policy giving federal investigative agencies the authorization to use publicly available social media information of individuals as a factor in determining eligibility of individuals being investigated for security clearance purposes. Investigative agencies can collect publicly available information from social media which pertains to the individuals associations, behavior and conduct which could impact the adjudication of an individual's security clearance.



Remember: What you post could potentially have a negative effect on your clearance.



REPORTING REQUIREMENTS

Because of your current position, you have been granted access to classified information that is vital to national security. You are responsible for safeguarding that information. Although it is an honor and a privilege to hold a security clearance, it also carries certain obligations that you must meet in order to maintain your access.

Because you hold a clearance it is your obligation to report to your security office various behaviors, incidents, or events exhibited by yourself or your coworkers that might in some way impact national security.

The following items are reportable:

FOREIGN TRAVEL, FOREIGN CONTACT, PERSONAL LIFE CHANGES, PSYCHOLOGICAL COUNSELING, FINANCIAL CONCERNS, COMPUTER/INFORMATION SYSTEM MISUSE, PASSWORD MISUSE, IMPROPER SECURITY PRACTICES, ALCOHOL-RELATED ISSUES, DRUG USE, CRIMINAL CONDUCT, SUSPICIOUS INCIDENTS



REPORTING REQUIREMENTS CONT.....

Foreign Travel: Report all foreign trips in advance in which a pre-travel defensive security briefing is requested/required or if travel is to a HOT SPOT country. If you're unsure if the country is a HOT SPOT then please contact your Security Officer.

- Business or personal travel (vacation, family emergency, etc)
- Report your trip in advance as necessary
- Follow up with your security office upon your return

Foreign Contacts:

A foreign national that an individual has continuing contact with may be a stranger, business/work associate, or someone quite close to you such as a significant other, persons you have an affectionate relationship with relative's spouse, or family friend.

- Any attempt by a foreign national to solicit sensitive/classified information or other contact that you regard as
suspicious
- Close and continuing contact with a foreign national in any capacity: in person, by telephone, via internet, etc.
- Contact with anyone who works for, or is associated with, a foreign government (including a foreign embassy) or
a foreign-owned organization or business
- Financial obligations to, investments in, or employment with foreign nationals and companies

REPORTING REQUIREMENTS.....

PERSONAL LIFE

CHANGES

- Change of name
- Change in marital status
- Change in cohabitation (involving a non-US citizen)


SUSPICIOUS INCIDENTS

- Personal Security
- Facility Security

FINANCIAL CONCERNS

- Excessive indebtedness
- Bankruptcies
- Garnishments
- Judgments
- Unexplained financial affluence

ALCOHOL-RELATED ISSUES

- Arrests
 - Treatment
 - Counseling
- 

REPORTING REQUIREMENTS.....

COMPUTER/INFORMATION SYSTEM MISUSE

- Unauthorized entry into an automated information system, whether government or contractor, for any reason
- Modification or destruction of hardware or software on any government or contractor equipment

PASSWORD MISUSE


- Obtaining someone else's password
- Sharing a password
- Using a password to browse through another's account without permission
- Copying/Deleting information on another's account without permission

CRIMINAL CONDUCT

- All arrests (regardless of whether or not there is a conviction)
- Knowledge of a criminal act by another accessed individual
- Knowledge of a criminal act by a member of your immediate family or close relative

REPORTING REQUIREMENTS...

IMPROPER SECURITY PRACTICES

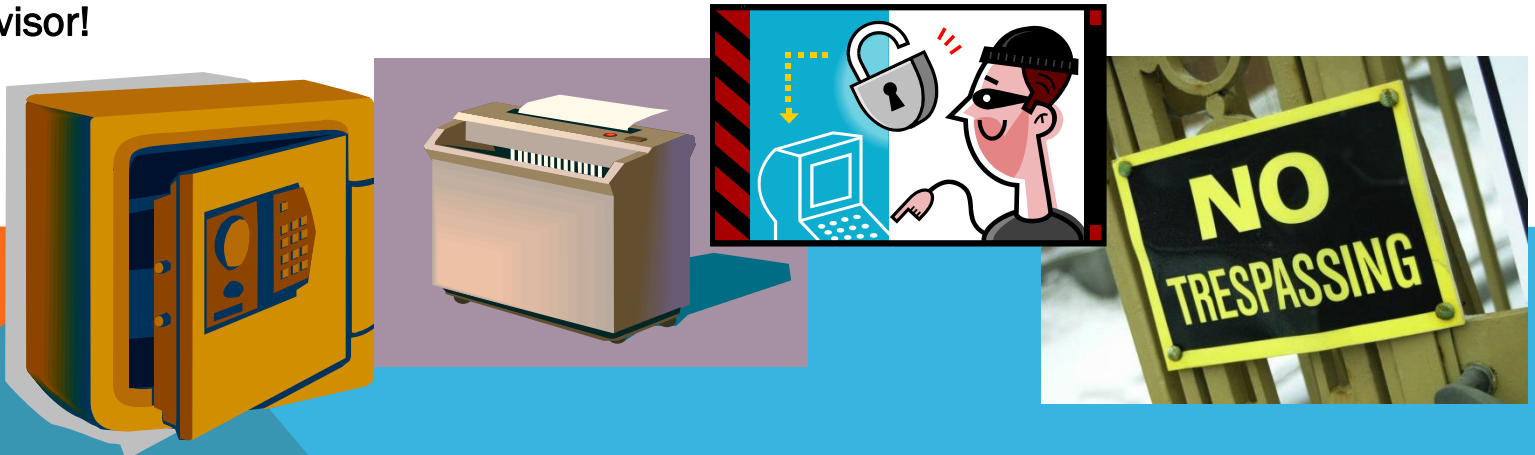
- Inadvertent or deliberate removal of classified information/materials to an unauthorized area
 - Inadvertent or deliberate unauthorized destruction of classified information/materials
 - Knowledge of a security violation or infraction & not reporting it
 - Deliberate or inadvertent disclosure of classified information/materials to an unauthorized person
 - Loss of classified information/materials
 - Requests for classified information/materials through unauthorized channels
- 

SECURITY VIOLATIONS AND DISCIPLINARY ACTION

It is incumbent upon all cleared employees to report violations, both those committed by them, and those committed by others (NISPOM 1-300)

No...this is not tattle-tailing! All cleared employees are required to protect classified information as a part of being granted a security clearance and **REPORT ANY SECURITY VIOLATIONS!!!**

Report any adverse information, incidents or suspicious acts to the FSO or your immediate supervisor!



PSYCHOLOGICAL OR SUBSTANCE ABUSE COUNSELING

Just so we're clear...
seeking help from a mental health professional will

NOT

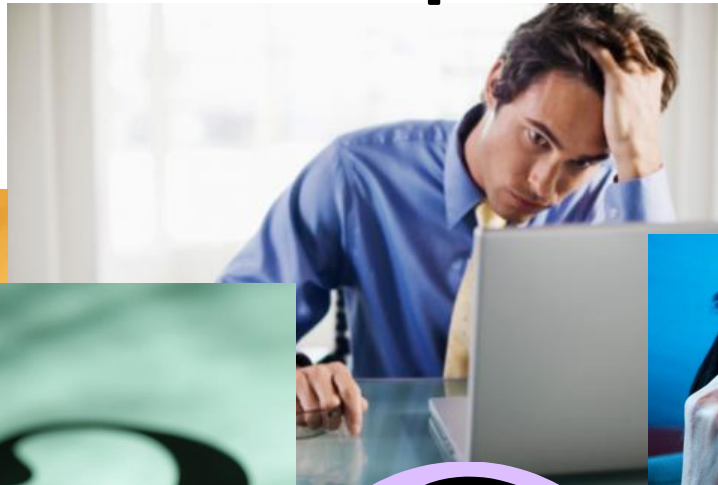
have a negative effect on your security clearance

The below psychological treatments are NOT reportable:

- For marital, family or grief counseling;
- Not related to violence by you;
- Strictly related to adjustments from service in a military combat environment.

REPORT, REPORT, REPORT

Remember when in doubt...
Still report it!!!!

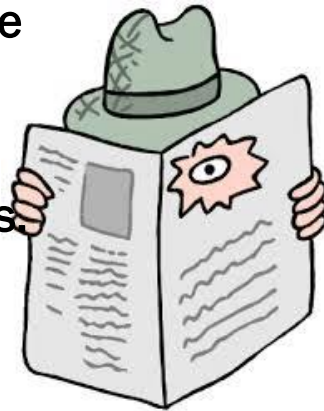


CONFIDENTIAL



ESPIONAGE

- You may be the target of foreign intelligence activity. Never think that “it couldn’t happen to me!”
- Foreign powers may seek to collect U.S. industrial proprietary economic information and technology, the loss of which would undermine the U.S. strategic industrial position.
- Foreign intelligence collectors are targeting US corporate marketing information in order to gather data that would help their respective countries.
- Overseas travel, foreign contact, and joint ventures increase your company’s exposure to the efforts of foreign intelligence collectors.



FOREIGN TRAVEL

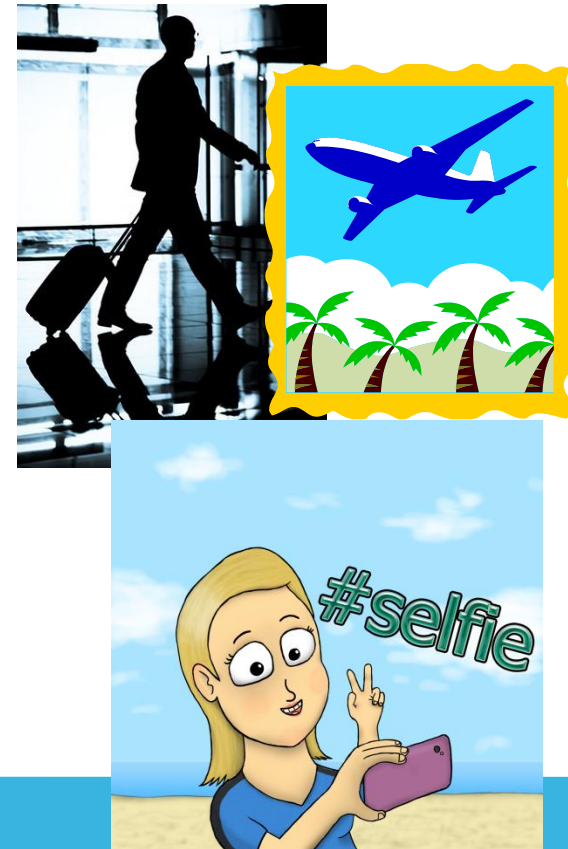
As a CCCR employee, you are responsible to:

Request a “Notification of Foreign Travel” form from the CCCR Facility Security Officer BEFORE you travel. Fill out this form and return it to CCCR Security BEFORE you travel!

Upon return from travel, your FSO will call to conduct a quick travel debrief.

Complete the “Foreign Contact Form” if you had contact and discussions with any foreigners that should be reported.

Questions?? Ask the Concord Crossroads Facility Security Officer!



STAYING SAFE WHILE ABROAD...

Plan and prepare well regardless if traveling for work or leisure.

Leave a copy of your itinerary with family or friends at home so that you can be contacted in case of an emergency.

Be Vigilante and always be aware of your surroundings and any one you may come in contact with on your trip.

Learn about the culture, customs, and laws of countries you visit.

A great resource is the Department of State website:
www.state.gov.

STAYING SAFE CONT'D...

Make sure you have a signed, valid passport and visas, if required. Also, before you go, fill in the emergency information page of your passport!

Make 2 copies of your passport identification page. This will facilitate replacement if your passport is lost or stolen. Leave one copy at home with friends or relatives. Carry the other with you in a separate place from your passport.

Do not leave your luggage unattended in public areas. Do not accept packages from strangers

Do not mention, discuss or even imply involvement in special or classified projects or activities.

Avoid moral indiscretions or illegal activity which could lead to compromise or blackmail.

Never attempt to photograph military personnel or installations or other restricted or controlled areas.

Contact CCCR security before leaving and upon return for your briefing/debriefing, as well as completing the proper forms. Incidents of an intelligence nature or foreign national contact must be reported. (Foreign national contact does not include incidental contact that occurs in a normal social context.)

Maintain a low profile; avoid attracting attention to any governmental affiliation.

Never make mention of your whereabouts on social media.



VISITS AND MEETINGS

Incoming Visit Authorization Requests

If you are planning a meeting that may discuss classified information, see the Security Manager at the Government Facility for visit requirements. Do not discuss classified information in a meeting without approval from FSO.

Outgoing Visit Requests

If you require a Visit to attend a meeting/conference, contact the Concord Crossroads FSO in a timely manner. Please provide the Dates of the Visit, The POC Name, Phone and Email as well as the SMO code for the facility.

DEFENSE HOTLINE INFORMATION



CONTACT INFORMATION

Bianca Dodson
Facility Security Officer
Concord Crossroads, LLC
2525 Pointe Center Court, Suite 350
Dumfries, Virginia 22026
703.670.8770 x314
703.634.2337 (FAX)

*****UPON COMPLETION OF THE PRESENTATION, PLEASE NOTIFY ME.*****

