2024 Initial and Annual Security Refresher Briefing

(As Of 6 Dec 2020)

Security Message

- The protection of Government and 9line's assets, people and property, both classified and controlled unclassified, is the responsibility of each and every member, regardless of how it was obtained or what form it takes. Our vigilance is imperative in the protection of this information. Anyone with access to these resources has an obligation to protect it.

- The very nature of our jobs dictates we lead the way in sound security practices. This security briefing provides a good foundation.

Briefing Objective

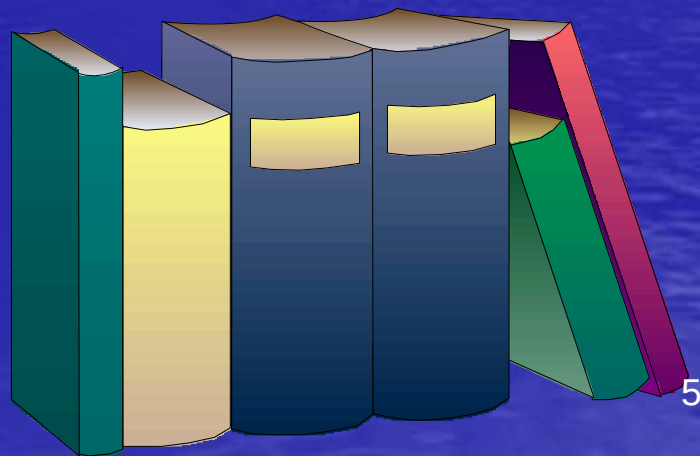
- This briefing will:
  - Identify your personal security responsibilities
  - Provide a basic understanding of NISPOM, DoD, and 9line's Security Standard Practice Procedures
  - Provide a brief understanding of Counterintelligence (CI), Insider Threat, and Cyber Security
  - Explain the importance of protecting government and company assets

Why Security?

- NISPOM, DoD, Supported Commands, and 9line's Security Programs are established to counter threats
- Threats to classified and controlled unclassified assets can include:
  - Insider (government employees, contractor employees, and authorized visitors)
  - Criminal and Terrorist Activities
  - Foreign Intelligence Services
  - Foreign Governments

Individual Responsibility

- You are responsible for:
  - Becoming familiar with local security regulations pertaining to your assigned duties
  - Notifying your security manager of changes in your status which could affect your security clearance, defined later in this briefing



9line's Facility Security Officer (FSO)

- FSOs – Contact David Heintz Jr, AFSO at (813) 892-8918 email david.heintz@9linellc.com
- After Hours – (813) 892-8918
- FSO will provide you with specific guidance on security matters.
- Your 9line Security Officer is your primary point of contact for all security issues/questions.
- It is important that you understand how your clearance and security procedures apply in connection to your duties.

Why Do We Classify Information?

- Information could be expected to cause damage to national security if subjected to unauthorized disclosure
  - **Confidential** - information, if released, could cause ***damage*** to national security
  - **Secret** - information, if released, could cause ***serious damage*** to national security
  - **Top Secret** - information, if released, could cause ***exceptionally grave damage***
    - SCI (Sensitive Compartmented Information) is not a classification level, but an access control system
- Information requires protection

Information Security

- Pertains to the *protection* of classified and sensitive information, to include but not limited to:
  - Marking
  - Handling
  - Transmitting
  - Storing
  - Destroying
  - Couriering

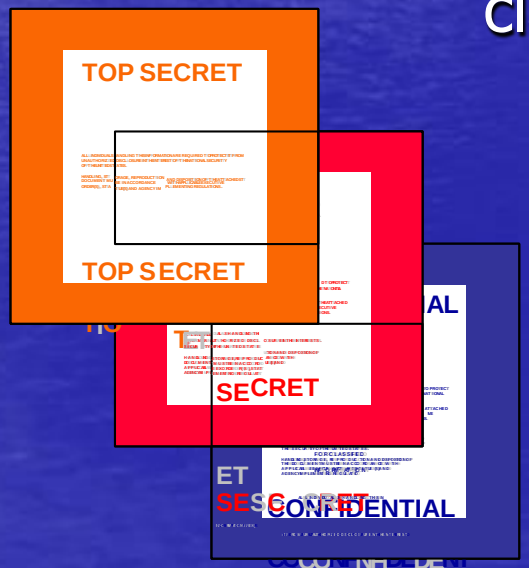
How Do I Identify Classified Documents?

?

CONFIDENTIAL (C)

SECRET (S)

TOP SECRET (TS)



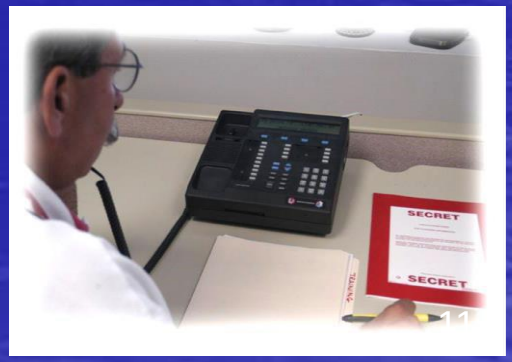
All classified information and equipment such as copiers/printers must be appropriately *marked* to alert potential recipients to the information's classification.

Marking Classified Information

- Purpose of Marking:
  - Alert the holder to the presence of classified information
  - Eliminate doubt of its required level of protection
- Markings apply to hard copy (documents) and soft copy (electronic) information
- All classified information must contain:
  - Portion markings (paragraphs, subject lines, etc.)
  - Page markings (top and bottom)
  - Overall markings (title page, first page)
  - Classification authority (derived from) and
  - Declassification instructions

Safeguarding Classified

- There are different measures and controls that are prescribed to protect classified information.
- Classified Information ***Must*** Be:
  - Under the control of or guarded by an authorized person or stored in a locked security container, vault, or secure room
  - Discussed on secure telephones or sent via secure communications
  - Discussed in an area authorized for classified discussion
  - Processed on approved equipment
  - Destroyed by approved methods



Use of Control Measures

- Classified material must be under constant surveillance and control when removed from a security container.
- Use cover sheets to alert the holder to the presence of classified material.
- Complete SF 702, Security Container Check Sheet, when container is opened, locked, and checked.
- Use Open-Closed, Open-Locked signs on security containers.
- Complete SF 701, Activity Security Checklist, at the end of every work day.
- Find out what else is required in your office to protect classified information from your Security Manager.

NOTE: 9line does not store classified at our facility but these procedures must be used at government or other sites where applicable. 9Line employees working at USSOCOM must follow the SOP for security at that site and must be trained on all procedures IAW with this SOP.

Telephone Security

- Discuss classified only on:
  - Secured Phone
  - Remember! STU-III phones are only secure when they have been switched to secure voice mode.

- When using a commercial phone, remember:
  - Do NOT discuss classified. Do NOT attempt to "talk around" the classified information
  - Terminate a call if the caller attempts to discuss classified
  - Be alert to classified discussions around you
  - Be aware that your non-secure phone call can be monitored!
  - Never discuss classified on a cell phone

END-OF-DAY CHECKS

- STU-III KEYS, STE CARDS SECURED

- IN-BOXES CHECKED

- DESK TOPS CLEAN
- CPU DRIVES REMOVED

- SECURITY CONTAINERS LOCKED

- CHECK & INITIAL SF-701

NOTE: 9line does not store classified at our facility but these procedures must be used at government or other sites where applicable. A clean desk policy will be used at our facility.

Classified material can be *ANY* of these:

Machinery, Documents,
Emails, Models, Faxes,
Photographs, Reproductions,
Storage Media, Working Papers,
Meeting Notes, Sketches, Maps, Products,
Materials, etc.

Access to Classified Information

ACCESS

The ability and opportunity to obtain knowledge of classified information. This can involve seeing, hearing, or touching classified information, material, or equipment.

=

CLEARANCE

Administrative action, usually involving a form of background investigation and adjudication determination.

+

SF 312

Classified Information Nondisclosure Agreement: All persons authorized access to classified information are required to sign a legal contractual agreement between you and the U.S. Government.

+

NEED TO KNOW

Determination made by an authorized holder of classified information that a prospective recipient requires access to perform a lawful and authorized government function.

Your Investigation and Clearance

- All DoD government and contractor personnel are subject to a background investigation.
- Investigations are conducted to determine suitability for a position of trust and / or granting of a security clearance.
- Your suitability is continually assessed.

  - Your position sensitivity and / or duties will determine your level of clearance.

Your Clearance Responsibility

A security clearance is an individual responsibility. It is in your best interest to make sure your clearance stays current.

Reinvestigations are required every 6 years for both Top Secret, and Secret clearances. The date is determined by the date your last investigation closed.

If the investigation has expired (6 years from the date the investigation was completed for TS and S) and you have not submitted a reinvestigation packet, your access to classified material will be downgraded to the next lower level until you complete a re-investigation packet.

The Continuous Evaluation (CE) Program was established to assist with the back log of reinvestigations. This program allows for more time in between reinvestigations. For example, if you were granted Secret clearance in 2015, enrolled in CE in 2020, you would not require a reinvestigation until 2026 (6 years from date enrolled in CE)

Personnel Security Information

Suspension of access can occur due to:

- Criminal, dishonest, immoral or notoriously disgraceful conduct and negligent or disruptive patterns
- Habitual or misuse of intoxicants (i.e. DUI's, DWI's, binge drinking, confirmed alcoholic, etc.)
- Drug abuse (i.e. use, possession and or selling of any illegal drug)
- Recurring financial trouble (i.e. failure to pay debts in a timely manner, history of writing bad checks, bankruptcy, living above your means, etc.)
- Mishandling of classified or sensitive material
- Misuse of government issued equipment, like phones or laptops (e.g. plugging a USB or anything into the laptop)

Personnel Security Information

Suspension of access can occur due to:

- Behavior, activities or associations which tend to show a person is not reliable or trustworthy
- Acts of reckless, irresponsible, or wanton behavior indicating poor judgment and or instability
- Falsification of information provided on security forms or information provided during the course of the investigative process
- Misuse of government computers (i.e. typing classified on unclassified system, pornography, etc.)

Make sure you report any of these incidents to your security officer as soon as they occur. Further reporting requirements follow:

Counterintelligence and Understanding the Threat

- CI seeks to identify and counter unlawful penetrators of cleared U.S. industry and stop foreign attempts to obtain illegal or unauthorized access to U.S. classified information and other sensitive data and technology.
  - Actors who may pose a risk include:
    - overly curious visitors, co-workers/insiders, friends or neighbors; and
    - foreign nationals, governments, or intelligence services;
    - other companies or competitors (industrial espionage);
    - anyone who seeks or attempts to access classified information without the appropriate clearance and "Need-to-Know"
- Commonly targeted items include critical military technology, proprietary company data, and national defense information which could also have an economic impact. See the Targeting U.S. Technologies report on the Defense Counterintelligence and Security Agency (DSS) website for more information (https://www.dcsa.mil/)

Protect yourself from CI Threats By:

–Be vigilant and use caution when traveling abroad, attending trade shows, or when meeting with foreign nationals.

–Receiving proper authorization on the release of sensitive or classified information.

- Report any attempt to access sensitive information from unauthorized person(s).
- If something seems suspicious, report it right away.

Insider Threat

- **Insider**: Anyone who has authorized access to company resources by virtue of employment, or contractual relationship with the company.
- **Insider threat**: A person with authorized access, who uses that access wittingly or unwittingly, to harm company interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.
- **Counter-Intelligence (CI) insider threat**: A person, known or suspected, who uses their authorized access to facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise information, or commit espionage on behalf of a Foreign Intelligence Entity (FIE).
- **Foreign Intelligence Entities (FIE)**: Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information; blocks or impairs U.S. intelligence collection; influences U.S. policy; or disrupts U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorists.

Indicators of Insider Threat

- Keep in mind that not everyone will have one or more of these indicators; however, previous Insider Threat cases have been found to include one or more of these behaviors:
- Performing unrequired work outside of normal duty hours
- Unreported foreign travel
- Engaging in illegal activity or asking colleagues to participate in illegal activity
- Attempting to access physical areas or information systems outside the scope of duties
- Unexplained absences from work
- Pattern of negligence when handling classified information
- Unreported Adverse Information
- Displaying unexplained affluence or sudden reversal in financial situation
- Suspicious foreign contacts
- Support to terrorist groups

Report it!

–It is important for all employees to understand and recognize suspicious behavior or activity. If you suspect a possible insider threat, indicated by the suspicious behaviors, collection techniques, and transmission procedures listed above, it is your responsibility to report it to your FSO. Please note, that reporting is anonymous. Know one will know you reported.

Cyber Security

It only takes one negligent user to unwittingly open the virtual door for the bad guys, potentially allowing access to our network and critical assets. Improve cybersecurity and reduce risk by understanding the following:

1) Any activity involving a 9Line Asset that is not:
   - Specifically related to 9Line business objectives or interests
   - Adding value to 9Line
   - Furthering the Company's mission
2) Personal use of 9Line assets is discouraged, including personal use of the Internet. Do not access personal bank accounts, social media sites, video streaming sites, etc.
3) Never install software for personal use on a 9Line asset (includes cellphones, laptops, tablets, etc.). If you need a certain program, submit a request IT request and they will install it.
4) Ensure that you understand and comply with 9Line's Cybersecurity policies.

Regardless if you have a security clearance or not, Cybersecurity is everyone's responsibility

Reporting Suspicious Emails

- To report a suspicious email, do the following for UNCLASSIFIED email on 9Line equipment only:
  - Do not open any attachments or click on any links inside the email
  - Expanding the email header for additional valuable information (for most recent editions on Outlook):
  - Click on Snipping Tool and take "Snip" of the picture
  - Save the image and send it to myself or Tracy and title the email "Suspicious email"
  - After sending the Snip of the email, go to the top right corner of your Outlook and click on the Report Suspicious Email Button (highlighted in red)
  - After you've clicked on the Report Suspicious Email Button, a message may pop up stating this comes from a trusted source, click "yes", if you suspect it is. The email will be sent directly to the cyber team and will be removed from your inbox.
  - Note: If you're sitting on a government site, ask the local security team how to report suspicious emails.

If you'll be working at a customer site, ask your project manager or onsite security how to report a suspicious email.

Reporting Requirements…

- **You Must Report:**

- Change of:
  Name
  Marital Status
  Citizenship

- If a member of your immediate family (or your spouse's immediate family) is a citizen or resident of a foreign country

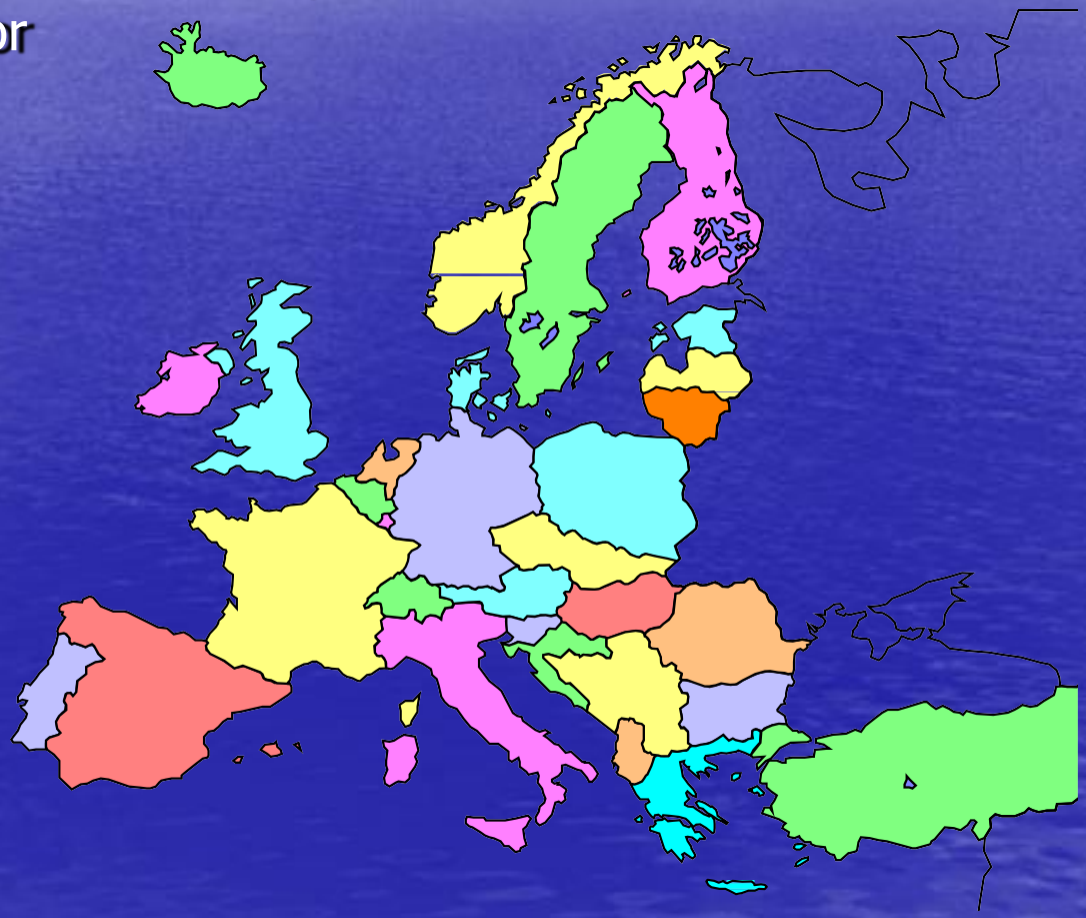
You Must Report…

- All continuing contacts with foreign nationals, to include shared living quarters and marriage
- Suspicious contacts with / by foreign nationals

- Foreign travel
- Official and Personal

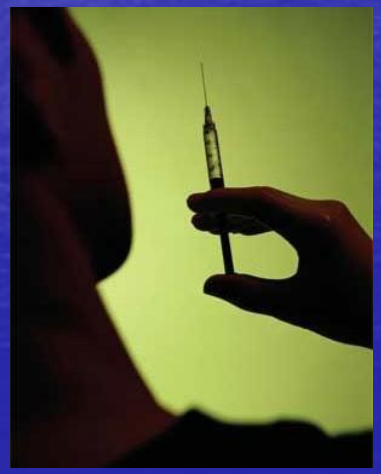
You Must Report…

- Any potential employment or service, whether compensated or volunteer, with a foreign government, foreign national, foreign organization, or other entity, or a representative of any foreign interest



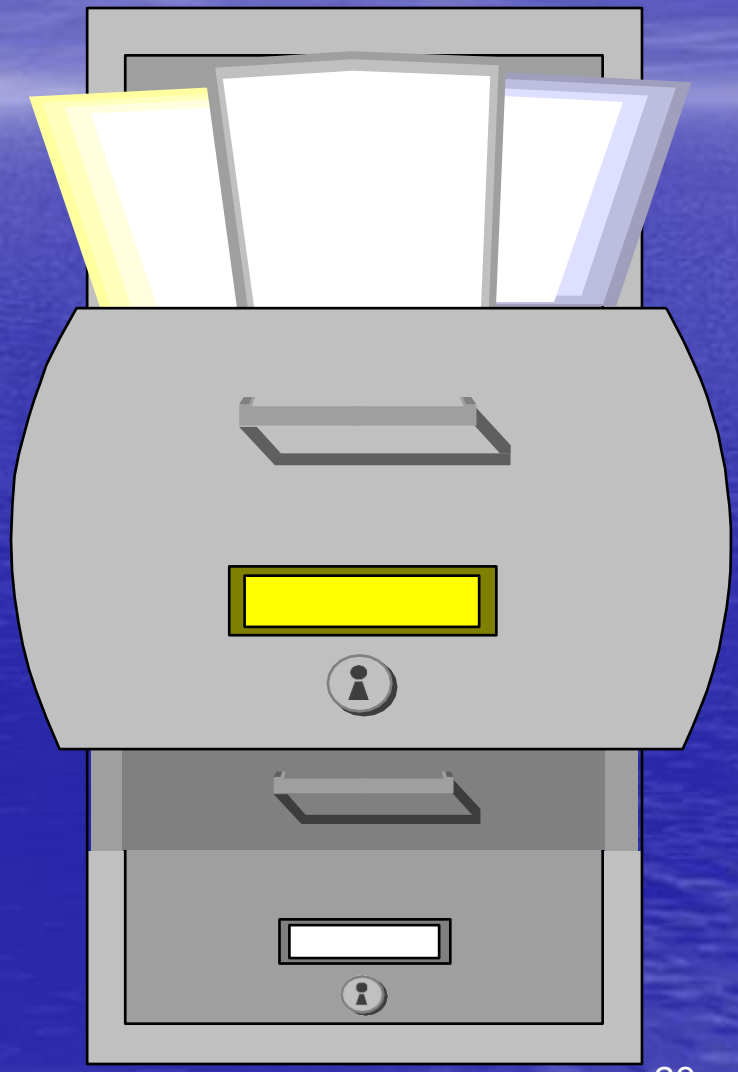
You Must Report…

- Adverse information concerning yourself or a co-worker that might have a bearing on their continued eligibility for access to classified information
- Adverse information includes, but is not limited to recent arrests, alcohol or drug related problems, and / or financial difficulties, etc



You Must Report…

- Loss, compromise, (or *suspected* loss or compromise) of classified information, including evidence of tampering with a security container used for storage of classified information
- Any security violation related to use of government equipment to include phones or government issued laptops.

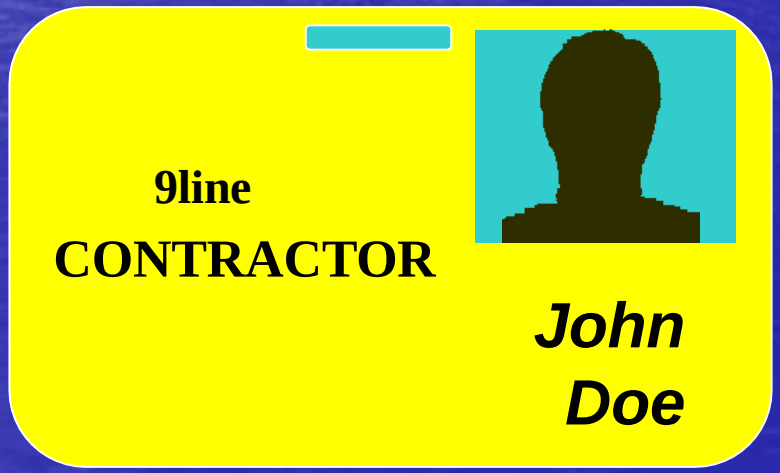


You Must Report …

- **Potential Espionage Indicators Exhibited by Others**
  - Unexplained affluence
  - Keeping unusual work hours
  - Divided loyalty or allegiance to the U.S.
  - Disregarding security procedures
  - Unreported foreign contact and travel
  - Pattern of lying
  - Attempts to enlist others in illegal or questionable activity
  - Verbal or physical threats
  - Inquiry about operations / projects where no legitimate need to know exists
  - Unauthorized removal of classified information
  - Fraud / Waste / Abuse of government credit cards and / or travel or training advances

You Must Report…

- A lost or stolen badge such as Command, or Common Access Card (CAC) must be reported immediately to Company or Command Security Managers



You Must Report…

- ANY TRAVEL OVERSEAS, 3 weeks prior to traveling, and you must do overseas travel training and review of security risks on the State Department web sites!

Command Badge and Visit Requests

- The 9line Security Team is responsible for verifying and submitting your security clearance to your work or TDY location security managers.

- As a 9line employee supporting Government contracts, you must represent yourself as a contractor employee when working or visiting Military, Federal, or other Contractor Facilities (i.e. not as retired Officer or Reservist).

You Must…

- Coordinate with 9line Security Team regarding additional security related briefings:
  - Initial & Annual / refresher
  - Insider Threat Program
  - Courier / hand-carrying classified
  - NATO
  - Visit Authorization Requests
  - Security debriefings
  - Out-processing requirements
  - Overseas Travel (personal or official)

- Be aware of other important training / awareness issues that follow:

Antiterrorism/Force Protection

- Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces.
- Actions taken to prevent or mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information.
- Training is required to be completed annually.

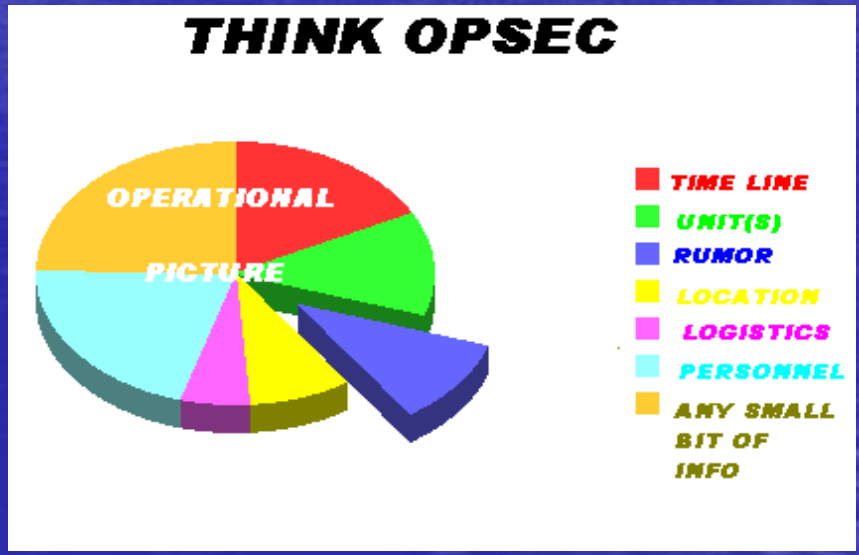
Information Assurance (IA)

- In the performance of your duties you will be required to have access to 9line and government computer systems.
- Information assurance protects and defends information and information systems by ensuring their availability, integrity, authenticity, confidentiality.
- You should participate in annual IA training inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.
- Comply with password directives and protect passwords from disclosure.

Operations Security "OPSEC"

- The achievement of surprise is essential to military effectiveness in both tactical and strategic operations. This requires continuous concealment of capabilities and intentions.
- Operations Security (OPSEC) is the protection of unclassified information that would reveal operational intentions.

- OPSEC is the principle means of achieving that concealment.
- Any small bit of information could help fit together an *operational picture*



Public Release of Information

- Public release of government information must be reviewed and approved by the Public Affairs Office, Freedom of Information Act (FOIA) Office, and 9line Security Office.
- 9line President is the only officer allowed to approve and release information.

You Can Make a Difference !

- Security is a team effort . . . .Your diligence in promptly reporting concerns and adhering to your agency's security policies and procedures will ensure the integrity of national security. As a team, we can protect our war-fighters, colleagues, and families from potential harm.

Good Security

- **Being Aware**
  - Know your responsibilities
  - Know your Security Officer
  - Know you surroundings
- **Being Careful**
  - Follow the rules
  - Pay attention to the details
  - Be responsible
- **Being Safe**
  - Stop, look, and listen to your surroundings
  - Ask questions
  - Report what needs reporting

Contact…

Your Security Team
With
Any Questions

Defense Hotline

- If you encounter a security violation or ethics issue, you have an obligation to either:
  - Report the incident to your 9line Security Officer
  - Use the Defense Hotline.

The Defense Hotline provides an unconstrained avenue for DoD and Contractor personnel to report without fear of reprisal. Defense Hotline, Pentagon, Washington DC, 1 800-424-9098

Acknowledgement

I certify that I have read and understand 9line's 2024 Annual Initial/Refresher Training Briefing.

Printed Name _____

Signature _____

Date _____