



Software Engineering
S E R V I C E S



SES ANNUAL SECURITY REFRESHER BRIEFING

January 18, 2014

GUIDING DIRECTIVE

Software Engineering Services is a Government contractor.

We are bound by the **National Industrial Security Program Operating Manual (NISPOM)** And Department of Defense (DoD) rules and regulations to properly protect and control all classified material in our possession.



You, as an employee, are equally bound under the law to provide the same protection and control.

What we'll cover...

- The investigative and adjudicative process
- Behavior that might jeopardize your clearance
- Personal activities that must be reported to your security officer
- Refresher of the basics
- The Threat
- Your security obligations and sources of help

A security clearance is a privilege, not a right.

- When you accept the privilege of access to classified information, you are also accepting the responsibilities that accompany this privilege.
- This is a lifelong responsibility.

Investigative and Adjudicative Process

- You were granted a security clearance after a two-step process:
 - **First step – the investigation.** Inquiry into your past to gather evidence to help determine whether you can be trusted with classified information.
 - **Second step – adjudication.** Decision whether to grant or revoke your clearance based upon the investigative evidence.

First Step: The Investigation

- Secret: National Agency Check/Local Agency Records Check (NACLC)
- Top Secret/SCI: Single Scope Background Investigation (SSBI)
- Conducted by the Office of Personnel Management (OPM)
- For SCI Access, the agency holding the SCI will conduct additional investigations as per internal guidelines.

Second Step: Adjudication

- A review of your record of behavior (favorable and unfavorable) against the 13 *adjudicative* guidelines.
- Guidelines are in place to ensure decisions are fair, impartial, and consistent.
- “Whole Person Concept” – Adjudicators
 - carefully weigh a number of variables
 - available, reliable information about you
 - both past and present
 - favorable and unfavorable

What makes the difference?

- Nature, extent, and seriousness of possible derogatory information.
- Did you voluntarily report the information?
- Were you truthful and complete in responding to questions?
- Did you seek help and follow professional guidance?
- Have you demonstrated positive changes in your behavior?

Example: Three years ago, as a result of a divorce, employee was faced with financial difficulties, resulting in an inability to meet all financial obligations in a timely manner. The employee has addressed the issues with his creditors and has been paying down his bad debt as agreed.



**SO, YOU'VE GOT YOUR CLEARANCE.
NOW, HOW TO KEEP IT!**

Standards of Conduct – The Guidelines

- To maintain access, you must recognize and avoid behavior that might jeopardize your clearance.
- Recognize behaviors in yourself or others that may need to be reported to your security officer and may signal that you or a co-worker may need assistance.
- **Early intervention** is often the key to quick, effective resolution of problems without harming you or the organization.
- Linked to the 13 adjudication guidelines.

Behavior that might jeopardize your clearance ...

13 Adjudication Guidelines

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Conditions
- Criminal Conduct
- Handling Protected Information
- Outside Activities
- Use of Information Systems

Recognizing and Reporting Behavior

- Exhibiting one or more of the described behaviors does **NOT** necessarily mean the individual is a security risk.
- Security judgment is based on pattern of behavior, not a single action. “Whole Person”
- If you are unsure, talk with your security officer or your supervisor.



SELF-REPORTING...KNOWING WHAT AND WHEN TO REPORT

REPORTING OBLIGATIONS



Things your FSO will want to know

Self- reporting on your Personal Activities

■ Change in Personal Status

- Marital status – married, divorced
- Cohabitation – living in spouse-like relationship; intimate relationship, engaged
 - SCI or certain Special Access Programs: report early, particularly if your partner is a foreign national
- Change of name

■ Foreign Travel

- SCI: Receive clearance for travel to hazardous countries
- Security Office will provide State Dept advisories on hazardous conditions and any known security concerns
- Receive a defensive security briefing

Self-reporting....

Foreign Contacts

- **Must report contact with individuals of any foreign nationality, either within or outside the scope of your official duties, in which:**
 - Illegal or unauthorized access is sought to classified or otherwise sensitive information
 - You may be concerned that you are a target of an attempted exploitation
- **SCI cleared individuals must report all close and continuing relationships with foreign nationals**

Self-reporting....

Loss or Compromise of Information

- Suspected or actual loss or compromise of classified or other sensitive information

First Priority: Regain control of the classified material

Self-reporting....

Adverse Information

Adverse information concerning yourself, a fellow employee, or a visitor. Adverse information is information which may indicate that permitting you access to classified, sensitive but unclassified, or proprietary information is not in the best interest of the U.S. or the Facility. This includes any recent convictions, arrests, drug or alcohol problems, major financial difficulties, etc.



Self-reporting....

Financial Problems

- Filing for bankruptcy
- Garnishment of wages
- Have a lien placed upon your property for failing to pay a creditor
- Eviction from a residence for failure to pay rent

Arrests

- Any, regardless of whether or not you were convicted or charges were dropped
- Other Involvement with the Legal System:
Target of legal action such as being sued

Self-reporting....

Psychological Counseling

- Psychological treatment is reported unless it is for marital, family, or grief counseling
- Strongly encouraged and endorsed
- Seeking help for routine life crises does not reflect adversely on an individual's judgment
- Viewed as a positive sign that an individual recognizes that a problem exists and is willing to take steps toward resolving it
- Does not jeopardize your security clearance

So, I report a personal problem, then what?

- **At some time in your life, you may face problems with inter-personal relationships, depression, alcohol, family issues, or similar difficulties**
- **Vast majority of those seeking professional help do not suffer damage to their career**
- **On the contrary, it enables one to get help with an unmanageable problem in order to get on with life**
- **Early intervention is often a key to early resolution**

Hey Ben, do you think anyone will report us for having just one beer at lunch?

Although they restricted themselves to only one beer at lunch time, Mike and Ben still found they were not at their most productive in the afternoons.



BACK TO BASICS.....

Don't monkey around with the basics!



Soft
S E

S

Protecting Classified

- Must never be left unattended
- Must never be discussed in public places
- Must only be discussed on secure telephones or sent via secure faxes
- Must be under the control of an authorized person
- Must be stored in an approved storage container
- Must never be processed on your computer unless approved by the U.S. Government

Telephone Security

- Discuss classified only on phones designated as secure
- 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!**

Disclosing Classified Information

It is **your personal responsibility** to know that the person you are dealing with is **both properly cleared and has a need to know**.

You must **never reveal or discuss classified** information with anyone other than those that are:

- **properly cleared**
- and
- **have a need to know.**

OPSEC and the Internet

“Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy.”

(Attributed to an Al Qaeda Training Manual)

How may the information you include in an e-mail or post on a web site help an adversary...?

- **Our intentions**
- **How we operate and our plans (CONOPS, OPLANS, SOP)**
- **Movement of forces**
- **Travel Itinerary**
- **Or simply the fact that your organization works with classified information or employs cleared personnel**

Threat Awareness ...



Information concerning troop rotations, locations, equipment, and technology is classified for a reason. Unauthorized release of this information can have a detrimental effect on the Warfighters' survivability.



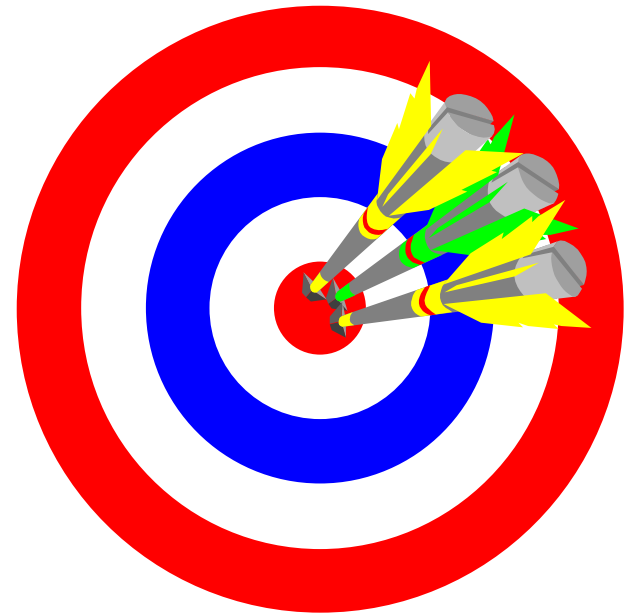


Software Engineering
SERVICES

THE THREAT

WE ARE A TARGET!

- We produce things of value to our adversaries
- Unauthorized disclosures will be very damaging - not only to the Government but also to our company
- To be competitive, we must be secure



THREAT TRENDS FOR 2012

- Increased collection attempts in 2012
- Facilitated by increased Internet availability and proliferation of company web pages
- 117 different countries were identified as collectors of our technology in 2012
- Countries collecting are those with modern economies and technology industries
- Collectors not necessarily going after complete weapons systems and military equipment

REGIONAL TRENDS FOR 2012

**East Asia
and the Pacific**

Near East

**South and
Central Asia**

**Europe
and Eurasia**



COLLECTOR AFFILIATIONS

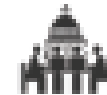
Commercial

Businesses in the commercial and defense sectors



Government Affiliated

Research institutes, laboratories, government-funded universities, or contractors representing a government agency



Government

Ministry of Defense, foreign military attachés, branches of the military



Individual

Persons seeking financial gain, persons avoiding traditional export procedures, or persons purportedly seeking academic or research information



Unknown

Instances when analysis could not directly attribute the contact to a specific end-user affiliation



MOST FREQUENTLY REPORTED METHODS OF OPERATION

Direct Request: Email requests, web-card purchase requests, price quote requests, phone calls, or marketing surveys

Foreign Visits and Targeting: Suspicious activity at a convention, unannounced visit to a cleared contractor, solicitations to attend a convention, offers of paid travel to a seminar, targeting of travelers, quotations beyond scope, or overt search and seizure

Solicitation and Seeking Employment: Offering technical and business services to cleared contractors, resume submissions, or sales offers

Suspicious Internet Activity: Confirmed intrusion, attempted intrusion, computer network attack, potential pre-attack, or spam

Exploitation of Relationships: Establishing a joint venture, official agreements, document peer reviews, scientific board reviews, foreign military sales, business arrangements, or cultural commonality

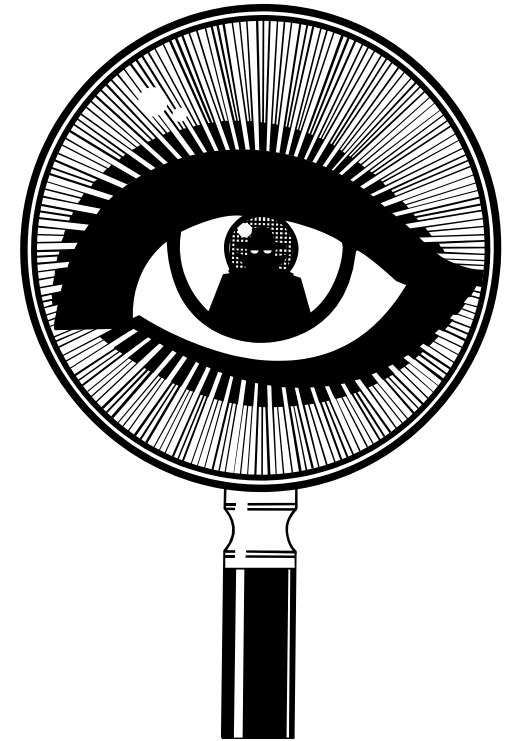
Other: Methodologies not otherwise captured above

TARGETED TECHNOLOGIES

- Information Systems
- Sensors
- Aeronautics
- Electronics
- Lasers and Optics
- Positioning, Navigation, and Time
- Marine Systems
- Armaments and Energetic Materials
- Ground Systems
- Materials and Processing Technology
- Space Systems

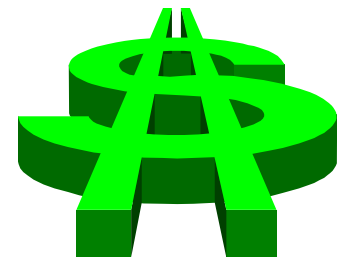
THE “TYPICAL” SPY

- **Seeks technical publications**
- **Attends scientific conferences and conventions**
- **Is not extraordinary**
- **Follows no rules of identification**
- **Anyone can be a SPY**



INDICATORS OF ESPIONAGE

- **Common indicators of possible espionage**
 - Unauthorized access, reproduction, removal of valued items
 - Frequent travel overseas
 - Exhibits extreme dissatisfaction with job, employer, U.S. government
 - Unexplained affluence



EFFECTIVE SECURITY COUNTERMEASURES

- Do not respond to suspicious foreign requests for information
- Refuse tours to unauthorized visitors
- Request additional information from foreign entities
- Question foreign entities about the reason(s) for their inquiries
- Refuse inappropriate visit sponsorship requests
- Use effective escorts to control visitors
- Apply security to web design and advertising



Software Engineering
SERVICES

YOU CAN NEVER B2 SECURITY CONSCIOUS

Bobbi Garcia shot this fabulous photo of the B2 high speed, low-level shedding condensation when she was flying chase on a recent mission. Her shot was awarded 1st place in Aviation Week & Space Technology's Military category.



What Are Your Security Obligations?

1. Maintain the trust placed in you
2. Protect classified, sensitive unclassified, and OPSEC information
3. Report: personal life changes, adverse information, contacts, loss or compromise, lost/stolen CAC or restricted area badge, potential espionage indicators, foreign residence, and foreign interests

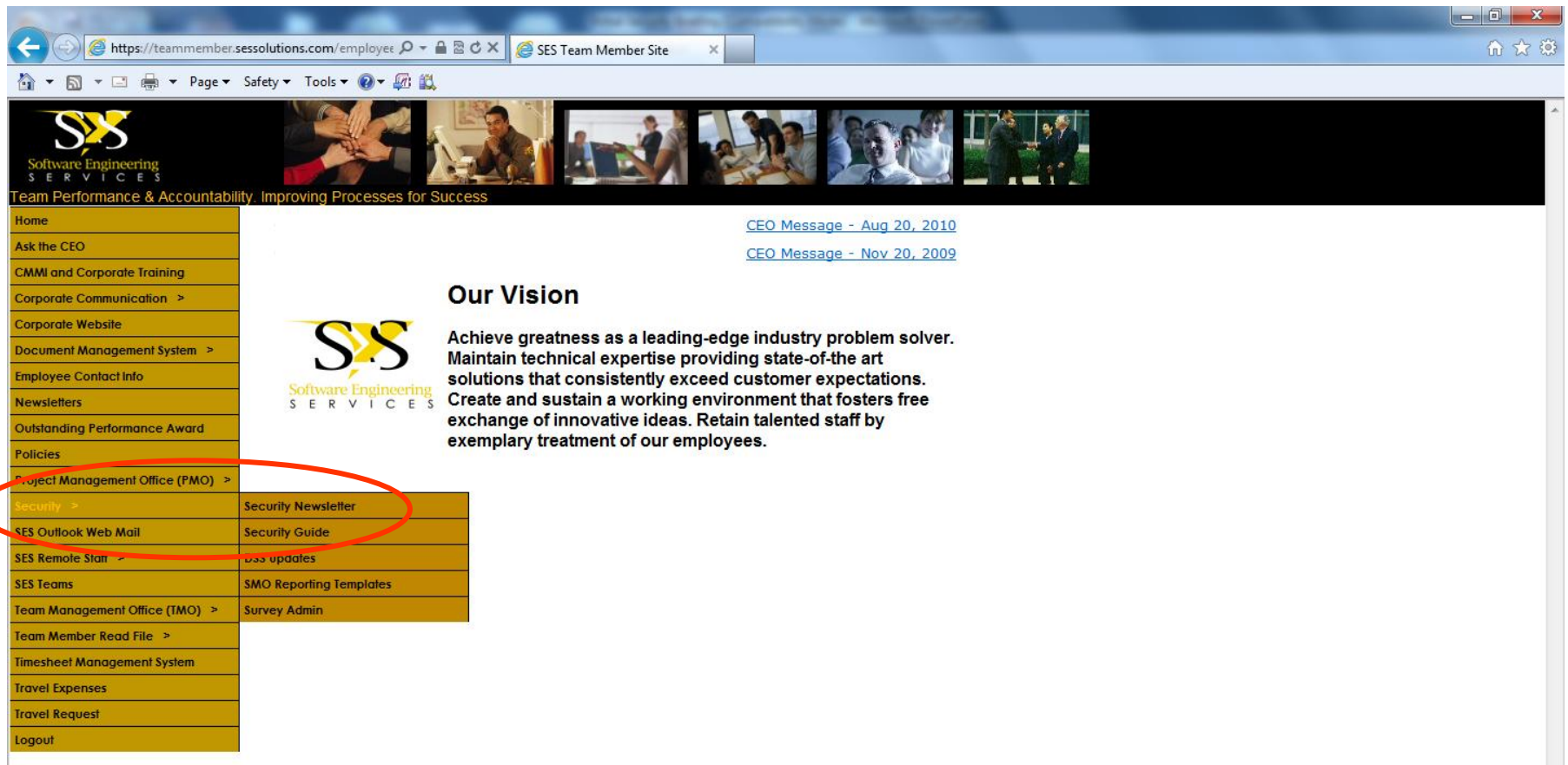
What Are Your Security Obligations? (Cont.)

4. Read SES monthly newsletters and report
5. Attend and report other government training
6. PMs of Classified Projects: Provide monthly security report

Protect the National Security of the U.S.

Sources Of Help

- NISPOM – DoD 5220.22-M
- **Security Newsletters** and **SES Security Guide** on the SES teammember website: <http://teammember.sessolutions.com>



The screenshot shows a web browser window with the URL <https://teammember.sessolutions.com/employee>. The page features a navigation menu on the left with the following items: Home, Ask the CEO, CMMI and Corporate Training, Corporate Communication >, Corporate Website, Document Management System >, Employee Contact Info, Newsletters, Outstanding Performance Award, Policies, Project Management Office (PMO) >, **Security >**, SES Outlook Web Mail, SES Remote Staff >, SES Teams, Team Management Office (TMO) >, Team Member Read File >, Timesheet Management System, Travel Expenses, Travel Request, and Logout. The 'Security >' link is circled in red. The main content area includes a header with the SES logo and the tagline 'Team Performance & Accountability. Improving Processes for Success'. Below this, there are two links for 'CEO Message - Aug 20, 2010' and 'CEO Message - Nov 20, 2009'. The 'Our Vision' section contains the SES logo and the text: 'Achieve greatness as a leading-edge industry problem solver. Maintain technical expertise providing state-of-the-art solutions that consistently exceed customer expectations. Create and sustain a working environment that fosters free exchange of innovative ideas. Retain talented staff by exemplary treatment of our employees.'

Questions???

- Talk to your Facility Security Officer (FSO)
 - Jim Moudry, 402-292-8660, ext 217
jmoudry@sessolutions.com
 - Sharon Lockhart, 402-292-8660, ext 210
slockhart@sessolutions.com (not yet, but soon)



BE AN ANGEL - SUPPORT OUR SECURITY PROGRAM

