ERC

Initial Security Briefing

Topics

- SF86 Information (e-QIP) Data Protection
- Non-Disclosure Agreement
- Threat Awareness
- Defensive Security
- Security Classification System Overview
- Employee Reporting Obligations & Requirements
- Security Procedures & Duties

ERC

Electronic Questionnaires for Investigations Processing (e-QIP)

As per the National Industrial Security Program Operating Manual (NISPOM) Section 2-202a.

The SF86 (e-QIP) questionnaire is subject to review solely to determine its adequacy and to ensure the necessary information has not been omitted. The information provided in conjunction with completion of the SF86 (e-QIP) will not be shared to any unauthorized personnel.

ERC

The Non-Disclosure Agreement

A lifetime contract between an individual and the U.S. Government, in which the individual agrees to protect U.S. classified information from unauthorized disclosures.

ERC

SF 312 – A Lifetime Contract

- Review ISOO SF 312 Briefing Pamphlet
- Things to remember:
  - Agreement may require review and approval of research material prior to presentation or publication
  - Agreement may limit your ability to freely discuss work with colleagues, relatives, friends.
  - Agreement may result in severe penalties if not upheld.

ERC

ERC

Threat Awareness

Foreign Intelligence Threat

- The gathering of information by intelligence agents in order to gain superiority
  - Intelligence Officers – trained by their own country to gather information
  - Spies – betray their own country by espionage
- Preventing this kind of betrayal is the ultimate goal of the entire U.S. personnel security system

ERC

The New Threat

- Traditional threat during Cold War era was the Soviet Union or Russia
- More countries are now involved (FBI estimates nearly 100), some of which were U.S. allies
- Espionage now involves not only the theft of classified information, but also high-technology information (both classified and not)
- Economic espionage is the acquisition by foreign governments or corporations of U.S. high-technology information to enhance their countries' economic competitiveness

ERC

The New Threat (Cont.)

- Economic espionage includes:
  - Basic R&D processes
  - Technology & trade secrets
    - Cost Analyses
    - Marketing Plans
    - Contract Bids
    - Proprietary Software
    - High-Tech Data

ERC

The New Threat (Cont.)

- Most vulnerable industries: biotechnology, aerospace, telecommunications, computer software/hardware, advanced transportation & engine technology, advanced materials & coatings (including stealth technologies), energy research, defense & armaments technology, manufacturing processes and semiconductors

ERC

Who are these spies?

Some Examples:

- Visitors on scientific exchanges, conferences, business tours
- Trade representatives or embassy liaison officers
- Foreign moles placed in American companies
- Students doing research in the U.S.
- Foreign hackers
- Disgruntled or greedy U.S. citizens

ERC

Warning Signs

- Attempts to gain access without a valid need-to-know or without required clearance
- Unauthorized reproduction or removal of material and secret destruction of documents
- Unexplained affluence
- Foreign travel on a regular basis without sufficient explanation
- Job dissatisfaction or deep grudges

ERC

Methods of Espionage

- Info openly available: Internet, commercial databases, academic and trade journals, company newsletters, annual reports
- Job interviews, hiring away knowledgeable employees, joint ventures or acquisitions, establishing a company in the U.S., “market research” surveys, pretext calling, moles, blackmail, bribery, consultants hired to spy on competitors (bugging, etc.)

ERC

The Damage

- Loss of lives
- Weakened or destroyed national defense
- Economic damage

ERC

Your Responsibility

- Recognize warning signs of espionage
- Report suspicions so that appropriate authorities can investigate the situation

ERC

Employee Reporting Obligations & Requirements

- Employees are required to report any contacts of a suspicious nature; adverse types of information; the possible loss, compromise or suspected compromise of classified information, and any change in employee status.

ERC

Suspicious Contacts You must report:

- Any efforts by an individual, regardless of nationality, to obtain illegal or unauthorized access to classified or sensitive unclassified information
- Any efforts by any individual, regardless of nationality, to compromise a cleared employee
- Any contact by a cleared employee with a known or suspected intelligence officer from any country
- Any contact which suggests an employee may be the target of an attempted exploitation by the intelligence services of another country

ERC

Adverse Information

- Cleared contractor employees are required to report adverse information regarding other cleared employees. Adverse information is that which reflects unfavorably on the trustworthiness or reliability of the employee to safeguard classified information.
- Examples of adverse information include: arrest for any serious violation, excessive use of alcohol or prescription drugs, any use of illegal drugs, bizarre or notoriously disgraceful conduct, sudden unexplained affluence, treatment for mental or emotional disorders, wage garnishments (except for court-ordered child support), etc.
- Be vigilant, but do not create an atmosphere of suspicion or intrusiveness in the workplace.

ERC

Adverse Information (Cont.)

- Anonymity is granted to the source
- Investigation is performed to validate the information
- Protection is afforded to the individual being investigated. The goal of reporting is to protect the individual from exploitation or persuasion to commit a security violation or espionage.
- Send reports and questions to your Facility Security Officer or alternate FSO. If this is not feasible, report directly to your company's DoD Defense Security Service Representative or The Defense Hotline. (See POC info at end of this presentation.)

ERC

Loss or Compromise

- Employees are required to report any loss, compromise or suspected compromise of classified information, foreign or domestic. Not reporting a known security compromise may, in itself, constitute a major security violation, regardless of the severity of the unreported incident.

ERC

Changes in Personal Status

- Changes in status of cleared employees that must be reported include:
  - Death
  - Change in name
  - Termination of employment
  - Change in citizenship

- See NISPOM Section 3 complete reporting requirements.

Other Reporting Requirements

- Any act of sabotage, possible sabotage, espionage or attempted espionage, and any subversive or suspicious activity.
- Employees are encouraged to report any attempts to solicit classified information, unauthorized persons on company property or any other condition that would qualify as a security violation or which common sense would dictate as worth reporting.

ERC

ERC

Security Classification System Overview

Classified Information

- NSI – National Security Information (classified information) is official government information that has been determined to require protection in the interest of national security.
- Forms of Classified Information:
  - Document, drawing, photograph, hardware, film, recording tape, notes, spoken words, etc.
- Material is classified by the originator, and the degree of safeguarding depends on its classification level

ERC

Classification Levels

- TOP SECRET: Information or material whose unauthorized disclosure could be expected to cause exceptionally grave damage to the national security
- SECRET: Information or material whose unauthorized disclosure could be expected to cause serious damage to the national security
- CONFIDENTIAL: Information or material whose unauthorized disclosure could be expected to cause damage to the national security

ERC

Other Categories of Classified Information

- RD: Restricted Data is Department of Energy data concerning design, manufacture or utilization of atomic weapons or nuclear material
- FRD: Formerly Restricted Data related primarily to the military utilization of atomic weapons.

ERC

Unclassified, but protected, information

- FOUO – For Official Use Only information must not be given general circulation
- Company private or proprietary information is not to be divulged to individuals outside the company
- SBU – Sensitive But Unclassified

ERC

Access to Classified Information - Two Conditions Must Be Met

1. The recipient must have a valid and current security clearance at a level at least as high as the information to be released
2. The recipient must demonstrate a genuine need-to-know (that the information is necessary for the performance of the individual's job duties on a classified contract or program), confirmed by the security representative.

It is the responsibility of the possessor of classified information to ensure the proper clearance and need-to-know of the recipient and must advise the recipient of the classification of the information disclosed

ERC

ERC

Safeguarding Classified Information

When Classified Is In Use:

- Safeguard materials at all times
- Classified information cannot be discussed/viewed over unsecured telephones, using unapproved computers, in public places or in any manner that may allow transmittal or interception by unauthorized persons.
- When working with classified material in an unsecured area: all curtains and doors should be closed. Protect classified materials from persons without appropriate clearance and need-to-know. Lock materials in approved safe whenever leaving the work area. Never take classified material home.

ERC

When Classified Is Not In Use:

- Properly secure in approved container or have it guarded by properly cleared person with a need-to-know.
- Approved containers should remain locked unless they are under constant surveillance and control.
- Shield combination from the sight of others when opening safe. The combination itself is classified at the same level as the material it is protecting.

ERC

Security Markings

- All classified material should be marked in a conspicuous manner by the originator of the material. See Marking Guide for additional information.
- If you discover unprotected classified information, provide protection and contact your Facility Security Officer immediately.

ERC

Reproduction of Classified Material

- No reproduction of classified materials is allowed without prior approval from the the individual or office responsible for classified document accountability.
- If reproduction approval is granted, copying can only be performed on properly approved machines
- Making “bootleg” copies of classified material is a serious, punishable offense.

ERC

Visitor Control Procedures

- Employees needing access to classified information at an outside facility must submit a Visit Request in advance of the visit.
- Visitors to our company requiring access to classified information must submit a Visit Request to the Facility Security Officer in advance of the visit.

ERC

Document Control Procedures

- If/when Company is approved for the storage of classified material.
  - No employee or visitor will be allowed to bring classified material in or out without first logging in the material through the Facility Security Officer.
  - If classified material will be needed at a facility to be visited, it will generally need to be sent ahead by the Facility Security Officer. (Hand carrying classified is rarely allowed and requires additional authorization and training.)

ERC

Classified Transmittal Within the Facility

- Ensure recipient has proper clearance and need-to-know
- Use hand receipts to track accountability
- Recipient should verify information contained on hand receipt is accurate
- Classified material should be double-wrapped and never left in an unattended mailbox.

ERC

Security Violations Policy

- Any perceived or suspected violation will be investigated to ascertain whether or not a compromise of classified material occurred. If a compromise is suspected, a report which identifies the party at fault must be submitted to the Defense Investigative Service. An adverse information report will also be filed in the responsible employee's records. Violations have a negative impact on both the employee and the company. Penalties are dependent upon the seriousness of the violation, the number of previous violations, and whether the violation was a deliberate act. Penalties may range from reprimand to termination, as well as potential civil and criminal proceedings.

ERC

Any Questions?

- Your Facility Security Officer:
  - Sean R. Doyle
  - 256-327-9155
  - seandoyle@erc-incorporated.com
  - security@erc-incorporated.com
- The Defense Hotline
  - The Pentagon, Washington, DC 20301-1900
    (800) 424-9098 or (703) 604-8569
- NASA Security Hot Line:
  - NASA Security Operations Center (SOC)
  - 877-627-2732

ERC