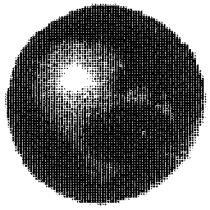
EXHIBIT 1

Global Linguist Solutions

ENCLOSURE (A)



INITIAL SECURITY BRIEFING

GLS Directorate Office of Security

UNCLASSIFIED

Defensive Security Message

The protection of U.S. Government assets, personnel (military/civilian) and property, both classified and controlled unclassified, is the responsibility of each and every member of GLS and its partner sub-contract companies.

We are all obligated to protect access to these resources regardless of how the assets are obtained or what form it takes. It is imperative to ALWAYS protect this information.

This initial security briefing provides a good foundation regarding local security policies, procedures, and corporate/individual responsibilities.

Purpose

- Identifies your individual personal security responsibilities
- Provides a basic understanding of security policies
- Explains the importance of protecting government assets and resources

Why Security?

- DoD Security Regulations, Directives and Programs are established to counter threats
- Threats to classified, sensitive and unclassified U.S. Government assets can include:
  - Insider (U.S. Government military/civilian personnel, contractor personnel and authorized visitors)
  - Criminal and Terrorist Activities
  - Foreign Intelligence Services
  - Foreign Governments

GLS Security Office

GLS PMO Security Department - Herndon:

- ☎ Leon Cliette – Sr. Manager of Security (703) 995-1391
- ☎ Linda Richardson – Facility Security Officer/CSSO (703) 995-1384
- ☎ Robert Wolf – Assistant Facility Security Officer/SSO: (703) 995-1366

GLS DEPCEN Security Department – Herndon:

- ☎ Joshua Finch – Security Lead (703) 995-1348

Physical Security

- Offers security-in-depth (control measures) and includes, but is not limited to:
  - ☑ Perimeter (surrounding environment)
  - ☑ Entry/Exit Inspections
  - ☑ Entry/Exit Control Points (Employee & Visitor Access)
  - ☑ Escorting
  - ☑ Badges and Common Access Cards (CAC)
  - ☑ Intrusion Detection Systems
  - ☑ Random guard patrols
  - ☑ Closed circuit video monitoring
  - ☑ Prohibited item controls

Your Individual Responsibilities

- Become familiar with local security regulations pertaining to your assigned duties and location
- Notify the GLS Security Office of changes in your status which could affect your security clearance; later defined in this briefing
- Report incidents to the GLS Security Office

Your Security Clearance

- Position sensitivity and/or duties will determine your level of clearance or access
- Three levels of security clearance are:
  - ☐ Top Secret
  - ☐ Secret
  - ☐ Confidential
- GLS Security personnel will provide you additional guidance regarding security clearance requirements

Your Investigation and Clearance

- All DoD Government (military/civilian) and contract personnel are subject to a background investigation, counter intelligence screening and polygraph examination
- Investigations are conducted to determine suitability for a position of trust and/or granting of a security clearance
- Your suitability is continually assessed
- You are required to coordinate with GLS Security Office regarding all security briefings, debriefings and/or out-processing requirements
- Refer to DoD 5200.2-R, DoD Personnel Security Program

CLEARANCE

Administrative action, usually involving a form of background investigation and adjudication determination granted by (DISCO) Defense Industrial Security Clearance Office

PLUS

SF 312

Classified Information Nondisclosure Agreement: All persons authorized access to classified information are required to sign a SF 312, a legal contractual agreement between you and the U.S. Government.

PLUS

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.

ACCESS

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

Information Security

- Pertains to the protection of classified and sensitive information.

- All individuals handling classified and sensitive information are required to protect it from unauthorized disclosure in the interest of U.S. National Security. Handling, storage, reproduction and disposition of these materials must be in accordance with applicable executive order(s), statue(s) and agency implementing regulations.

Example: classified documents will have the "Classification Markings" on its coversheet on the top and bottom of the document. Sensitive documents will have the "Privacy Act of 1974" disclosure statement, "FOUO" markings or DD Form 2923 coversheet.

Security Classification System

There are THREE levels of Classification:

- ☐ **TOP SECRET**

Exceptionally Grave damage to the National Security

- ☐ **SECRET**

Serious damage to the National Security

- ☐ **CONFIDENTIAL**

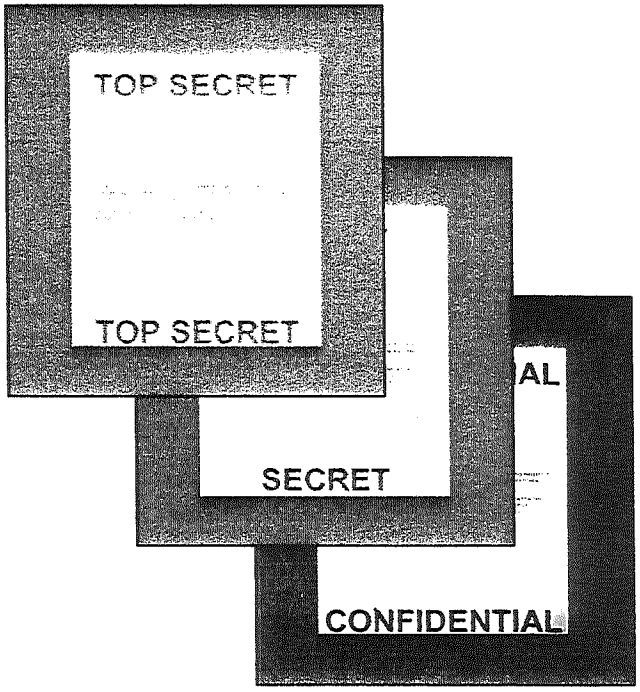
Damage to the National Security

Classification Markings

TOP SECRET (TS)

SECRET (S)

CONFIDENTIAL (C)



All classified information must be appropriately marked to alert potential recipients to the information's classification

Classified Material

- Here are some examples of different types of classified materials. All of which must still be properly marked and identified:
  - ☑Machinery
  - ☑Documents, emails and faxes
  - ☑Photographs, sketches and models
  - ☑Meeting notes, working papers, reproductions, storage media, thumb drives, maps, and products
  - ☑Substances or materials

Classified Information

- Must be under the control of an authorized person ***OR*** stored in a locked security container, vault, secure room, or secure area
- Must be discussed on secure telephones or sent via secure communications
- Must be processed on approved equipment
- Must be destroyed by approved methods
- Must be discussed in an area authorized for specified classified discussion(s)

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 personnel and family members, resources, facilities and critical information

Information Assurance (IA) & Responsibilities

- In the performance of your duties, you may be required to have access of government computer systems
- Information assurance protects and defends content information and its systems by ensuring their availability, integrity, authenticity and confidentiality
- Participate in annual computer security 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 or pass-phrase policy directives and protect passwords from disclosure

Public Release of Information

- Public release of information regarding GLS and its partner sub-contract companies, operations, and mission activities (pertaining to any/all U.S. Government Information) must first be reviewed and approved by the GLS Public Affairs Office.

Operations Security (OPSEC)

- OPSEC is a systematic process used to mitigate vulnerabilities and protect sensitive or critical information
- OPSEC awareness is a living program that must adapt and flex to the needs of GLS, its mission objectives and changing climate
- OPSEC does not replace other security disciplines – it supplements them!

Reporting Requirements

- Change in status
  - ☑ Name Change
  - ☑ Marital Status
  - ☑ Citizenship
- Adverse information
  - ☑ Yourself or co-worker
  - ☑ Arrest or Detention
  - ☑ Alcohol/Drug related issues
  - ☑ Financial difficulties
  - ☑ Loss, compromise (or suspected) of classified information
  - ☑ Suspicious contacts
- Foreign & Stateside Travel PTO & Reporting
- Continuing contacts with foreign nationals, to include shared living quarters/residency, marriage, and citizenship
- Representative of a foreign interest
- Lost/stolen badge or Common Access Cards (CAC)
- Fraud, waste & abuse
- Potential espionage

YOU can make a difference

As a team, we can protect our war fighters, colleagues and family members from potential harm. To ensure the integrity of U.S. National Security is maintained and preserved, be diligent by reporting concerns immediately and adhering to security policy and procedures.

Security Regulations

- Reference Security Regulations (not all inclusive)
  - Executive Order 12829, National Industrial Security Program
  - Executive Order 12958, as amended, Classified National Security Information
  - Executive Order 12968, Access to Classified Information
  - DoD 5200.1-R, DoD Information Security Program
  - DoD 5200.2-R, DoD Personnel Security Program
  - DoD 5200.8-R, DoD Physical Security Program
  - DoD 5205.2, DoD Operations Security Program
  - DoD Directive 5220.22-M, National Industrial Security Program
  - AR 25-2, Information Assurance

Further questions, please contact

Global Linguist Solutions

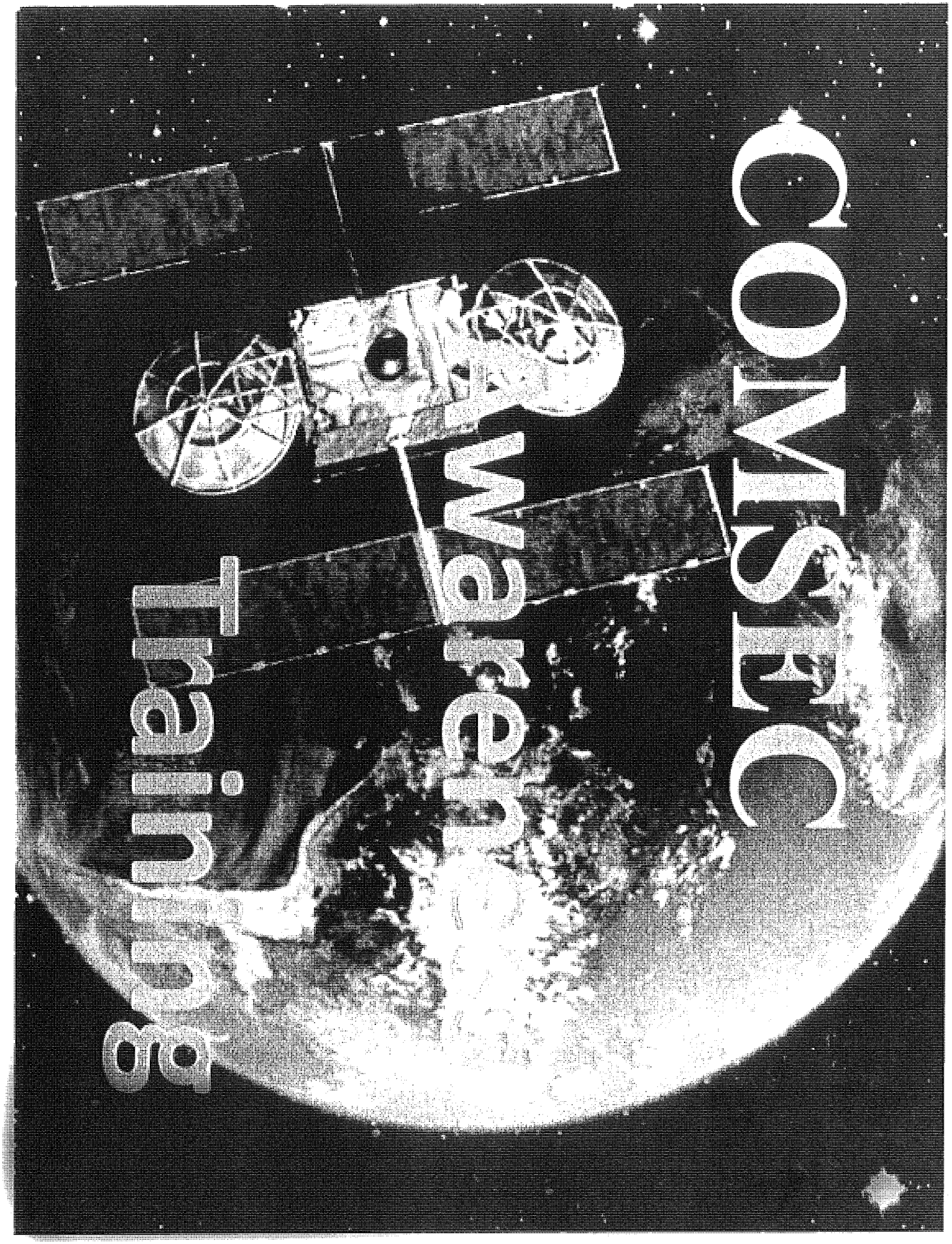
Linda Richardson
Facility Security Officer
VOIP (703) 995-1384

email: linda.richardson@gls-1.com
www.gls-corp.com

Questions and Answers

This concludes your Initial Security Briefing – Thank You!

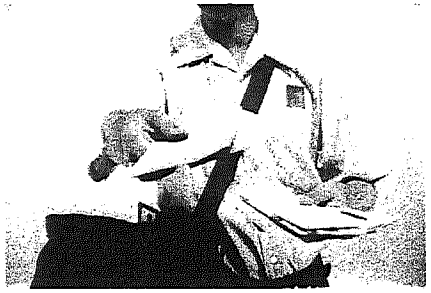
EXHIBIT 2



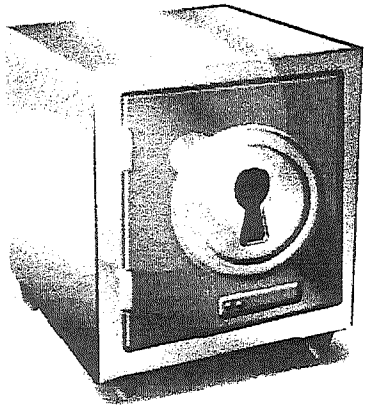
ENCLOSURE ( )

Why Are You Here Today?

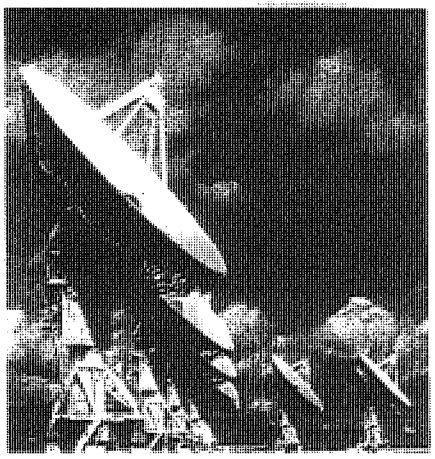
- You are here because your position with GLS requires access at some level to Communications Security (COMSEC) information, materials and systems. It is important that you understand the regulations concerning the safeguarding of these items and the consequences you can face if COMSEC is willfully disclosed to unauthorized persons.
- COMSEC is important because it the overall process used to protect Classified and other Sensitive (FOUO, CUI) information when it is passed from one person to another.



Transmission Security



Physical Security



Emission Security

Transmission Security includes all COMSEC measures taken to protect information from interception & exploitation while being electronically transmitted.

TYPES OF TRANSMISSION

Radio The most widely used form of electronic transmission. Since radio signals are sent out through the open air, they are one of the least secure methods.

Landline Phone The most convenient form of communication, and both voice and data can be transmitted. Since phone lines are easily tapped, this method is unsecure.

Cell Phone Very popular and widely used. This method is less secure than a landline phone as the signal is sent through the open just like radio signals.

Email Very popular and widely used. Has become one of the greatest risks to the security of Classified and Sensitive information. Messages sent through email are stored on company servers and remain long after a user has deleted them.

TYPES OF TRANSMISSION (Continued)

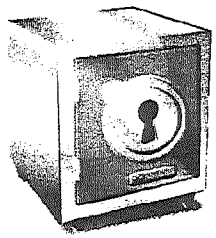
Face to Face

Hand Delivery

If you discuss information verbally or exchange a hardcopy version, COMSEC is required. The security of both these methods of transmission is totally dependent on the parties communicating.

US Postal & Courier Services

Can be used to transfer Sensitive and even some Classified information through Registered (SECRET) and Certified (CONFIDENTIAL) Mail or hand delivered by bonded couriers. In most cases, this is a very secure means of communication, but is not that useful if the information is urgent or there are time constraints.



Physical Security includes all COMSEC measures taken to physically safeguard all Classified and Sensitive materials/information.

Proper use of Storage Facilities & Security Containers

All Military/Government Contractors must comply with their Controlling Authority (DoD, DSS, NSA) when it comes to securing information. When assigned to a Military Unit/position that grants you access to Classified, Sensitive or other COMSEC information, make sure you are briefed on all organization-specific storage requirements.

Access

Use methods such as Badges, Guards and Alarm Systems to ensure only authorized persons have access to Classified, Sensitive or other COMSEC information.

Handling & Accountability

All Classified and Sensitive materials must be inventoried and accounted for on a continuous basis. When materials are removed from storage, the person removing them must maintain positive control or surveillance over them. When the task is complete, the materials should be returned and the container secured.

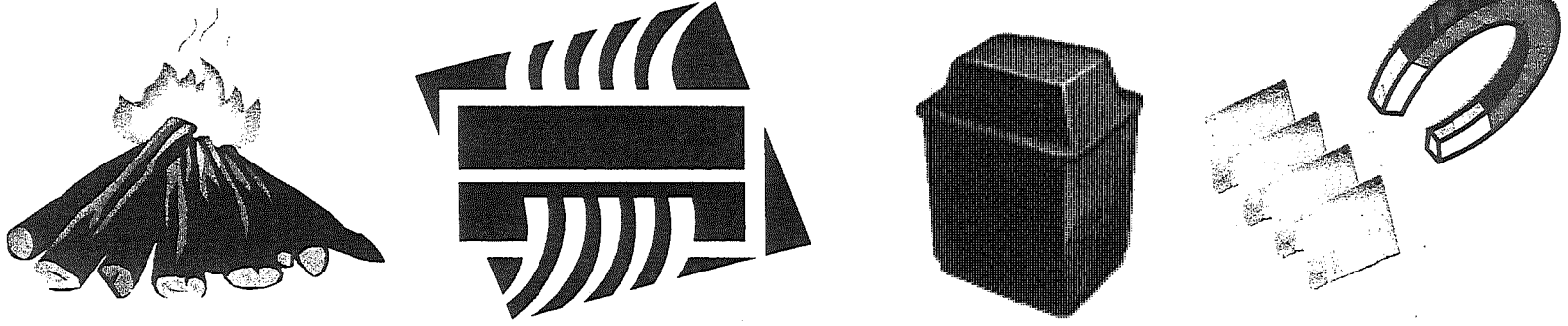
HOWEVER IMPORTANT THE TASK IS, NEVER TAKE SECURE MATERIALS HOME/TO YOUR CHU!!!

PHYSICAL SECURITY(Continued)

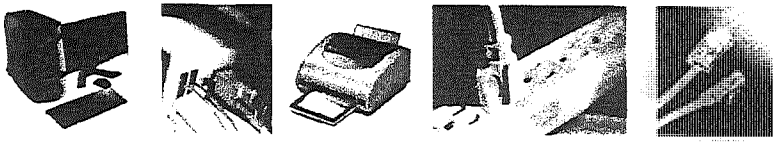
Destruction/Disposal

Most of you will never be in a position where you will be the one to destroy Classified materials and will simply place them in a burn bag or other receptacle for someone else. However, you may be asked to dispose of Sensitive or other COMSEC materials.

Approved Methods of Disposal



Emissions Security includes all COMSEC measures taken to deny unauthorized persons Classified, Sensitive or other information taken from captured emanations.



TEMPEST

All electronic equipment produces and radiates radio frequency signals, which can be captured and monitored by outside sources. TEMPEST is the process of gathering that electromagnetic output and reconstituting the original data to provide intelligence information to unauthorized persons.

Red/Black Separation

This is the act of maintaining distance or installing shielding between circuits and equipment that are designated to handle unencrypted Classified information and those designated for encrypted signals or normal unsecured communications use. Distance keeps electromagnetic voice/data information traveling along one line from 'bleeding' over into the other. Shielding does this as well, but also blocks the emanations from escaping.

SCIF

It is also possible to shield off a room or entire floor of your building for the purpose of working with highly Classified information or materials. These areas are known as Sensitive Compartmented Information Facilities. The regulations concerning SCIFs are strictly enforced and the process of accreditation is so demanding that most nonmilitary organizations (e.g. Government Contractors) do not possess one.

Information Classifications and Designations

Top Secret

This classification is given to information that if lost or compromised, would cause exceptionally grave damage to the security of the United States.

Secret

This classification is given to information that if lost or compromised would cause serious damage to the security of the United States.

Confidential

This classification is given to information that if lost or compromised would cause damage to the security of the United States.

For Official Use Only (FOUO)

This designation is given to information that if lost or compromised would pose a threat to the operations or mission of the Classifying Agency. (e.g. DoD, CIA) Although FOUO is unclassified, it is exempt from mandatory release under the Freedom of Information Act.

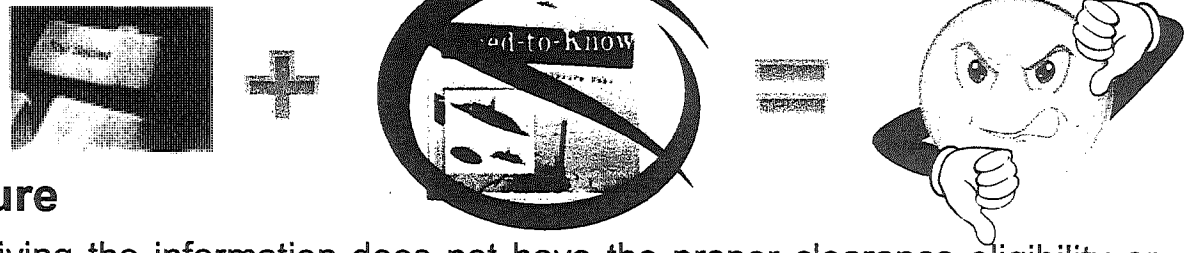
Controlled Unclassified Information (CUI)

This designation is given to information that if lost or compromised would pose a threat to the operations or mission of the controlling agency.

Disclosure of Information

Authorized Disclosure

Disclosure of Classified, Sensitive or other COMSEC information is authorized only when the party receiving the information has the proper clearance eligibility, can be properly identified and has the Need to Know.

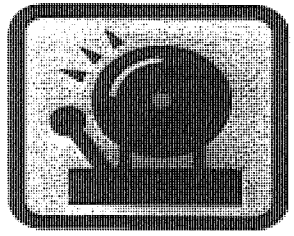


Unauthorized Disclosure

Happens when the party receiving the information does not have the proper clearance eligibility or Need to Know. In most cases, unauthorized disclosures are **unintentional**.

- **Lack of situational awareness in the outside world.** Discussing Classified, Sensitive or other COMSEC information when unsure or unaware of your surroundings can quickly lead to this information being disclosed to the wrong people.
- **Awe of Position.** High level management or higher ranking Officers/NCOs do not automatically have the Need to Know by virtue of their position or clearance eligibility. We all want to please our boss and work very hard each day to do so. Your boss must meet the same requirements for access to Classified, Sensitive and other COMSEC information as everyone else.
- **Trapped by Time.** Whenever we feel rushed or have a deadline we might not make, we tend to cut corners. When working with Classified, Sensitive or other COMSEC information, the job must be done by the book each time, every time—no matter how far it pushes us past the deadline.
- **Emotional Hazard.** Emotions play a large part in our lives and affect us on a daily basis. When we let emotions cloud our thinking the Classified, Sensitive or other COMSEC information we are working on is at risk of unintentional disclosure.

Security Incidents



Events that may jeopardize the security of Classified, Sensitive or COMSEC materials.

Personnel

These are acts of espionage or sabotage, or the willful disclosure of information to hostile or foreign agents by personnel having authorized access to the information.

Physical

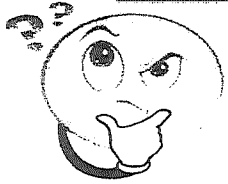
These occur when the control over Classified, Sensitive or COMSEC equipment, materials or information is lost.

Cryptographic

These are willful and unlawful actions/inactions that place any element of a Cryptosystem in jeopardy of compromise.

- Secure Telephone Units (STU)
- Secure Terminal Equipment (STE)
- Secure Voice Over-Internet Protocol (SVOIP)
- Secret Internet Protocol Router Network (SIPRNET)

SECURITY INCIDENTS (Continued)



➢ **Report Immediately!** If you become aware of a Security Incident, report it to your FSO/SSO/SMT. Try to answer the Five W's (Who, What, When, Where and Why?) for the initial report. Be careful to not include any Classified, Sensitive or other COMSEC information as you will most likely be transmitting using non-secure methods.

➢ **Correct the Problem.** This depends on the incident and your ability to correct it.

EX1. You find a file marked TOP SECRET stored in a container marked SECRET

EX2. You see a coworker using a thumb drive to copy MilAIR manifest times from a SIPR computer and then moving to a NIPR computer and emailing the file using Yahoo.

➢ **Participate.** There will most likely be an investigation after a Security Incident. Make yourself available to answer any questions asked of you regarding what you saw.

SELF-REPORTING IS ENCOURAGED

Preventive Measures

Changing Procedures

Changing Personnel

Arrest and Conviction

This can be anything from revising your Access Roster for Classified materials to requiring your employees to wear badges and provide escort for all non-company personnel in your building.

The Military will give you one opportunity (your first one) to work with them on Classified, Sensitive or other COMSEC materials. The consequence of a Security Incident usually means you are released from that unit and possibly the contract.

Depending on the severity of the Security Incident, jail time may be warranted for those involved. The loss, compromise or willful disclosure of Classified information carries its own punishments in addition to those from the Security Incident.

Conclusion

This concludes the COMSEC Awareness Training. Please complete your COMSEC Access Briefing Cert and send to GLSSecurity@gls-1.com

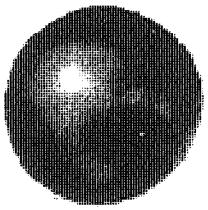
If you have any further questions with regard to the protection of Classified, sensitive or other COMSEC information and materials, contact your FSO/SSO

SSO
Kerry Superville
VOIP 703.840.1361 x 40134
SVOIP 709.241.1911
kerry.superville@gls-1.com

FSO
Linda Richardson
703.995.1384
linda.richardson@gls-1.com

AFSO
Bob Wolf
703.995.1366
robert.wolf@gls-1.com

Global Linguist Solutions



DEFENSIVE TRAVEL BRIEFING

GLS Directorate Office of Security

Purpose

- Defensive Travel Briefing is required by Department Administrative Order 207-1

- Presidential Decision Directive, NCS-12 "Security Awareness and Reporting Foreign Contacts"

- Establish and maintain Security Awareness Programs
- Understand your individual role & responsibilities to protect that information
- Awareness to vulnerabilities of Foreign Travel
- Acknowledge access to critical government information
- Focus on intelligence gathering threats

Area of Interest

- Export Administration Act
- Trade Issues
- Economic Indicators
- Industrial Resources
- Production Capabilities
- Manufacturing
- Critical Technologies
- Satellite Data
- Telecommunications & Computer Science Information
- Access to Facilities
- Access to Information
- YOU

National Security Threat List

- A threat to our national security is any intelligence activity regardless of the country which is:
  - ❑ Targeting U.S. Intelligence, Foreign Affairs Information and U.S. Government Officials
  - ❑ Directed at critical technologies
  - ❑ Collection of U.S. industrial proprietary economic information
  - ❑ Collection of information relating to defense establishments & national preparedness
  - ❑ Proliferation of special weapons of mass destruction

Prior to Departure

- Before going on PTO, you are required to report all Foreign and Stateside PTO travel to the Security Office
  - Subject Interview (SI) may accord while on PTO in the USA or at CRC before you deploy. You may be contacted by an investigator when the government is ready to conduct your SI.
- Contact the Security Office or Site Manager for travel advisories OR
- Department of State for recorded messages
  - ☑ Within the United States or Canada, call (888) 407-4747
  - ☑ Outside the United States or Canada call (202) 501-4444

Departure

- Avoid carrying corporate proprietary letters or documents (for official/unofficial use) or business packages. You may be viewed as a courier. Use approved/authorized method of delivery.

- NEVER carry classified materials with you! Always use the proper channels.

- When taking PTO travel to any foreign countries carefully complete visa applications for entry/exit purposes and Customs inspections.

- Do not carry any political, propaganda or pornographic materials which may be viewed as controversial, offensive or prohibited items.

Departure

- Prescription drugs should be clearly marked with your full name and expiration date.
- Limit the amount of ID cards you take with you. Keep records of what you do take and record serial numbers. Coordinate with CRC for your packing list and required documents.
- If you transport a laptop computer or smart phone device with you need to complete a TMP Form (Temporary Import, Export and Re-exports Form). These hand-carried items fall under the scope of the Export Administration Regulations and do not require a license under the authority of the tools-of-the trade provision of License Exception TMP (EAR Part 740.9 (a)(2)(i)).

Upon Arrival

- When on PTO travel is taken to any foreign countries more than 10 days, it is strongly recommended by the Department of State that you contact the local U.S. Embassy or Consulate; provide your local address and anticipated length of stay.
- Declare all money and valuables
  - ☑ Retain declaration slips
  - ☑ Keep receipts of all money exchanges
  - ☑ Declare cameras, radios, electronics, etc…
- Undeclared items are subject to confiscation upon departure
- While on PTO travel use of public transportation is typically recommended. Travel accommodations are generally arranged for official business or temporary duty assignments.

Your Activities and Behavior

- As a general rule of thumb, ALWAYS practice good OPSEC/COMSEC and Security Awareness habits at all times!

- NEVER discuss classified, sensitive or official business information in:
  - ☒ Hotel rooms, lobbies or reception areas
  - ☒ Vehicles (taxi cabs, buses or chartered)
  - ☒ Restaurants or other public areas
  - ☒ Emails, socials web pages, blogs, instant messages or mail

- Maintain a low profile
  - ☑ Always use best judgment
  - ☑ Never engage in illegal activities
  - ☑ Avoid excessive drinking
  - ☑ Use caution if gambling

Activities and Behavior

- Physical surveillance is better ignored than evaded
- If you locate possible surveillance equipment:
  - ☑ DO NOT try to neutralize or dismantle
  - ☑ Contact the local U.S. Embassy or Consulate
  - ☑ Contact GLS Security Office upon your return and REPORT the incident
- NEVER leave your briefcase or documents unattended in hotel rooms or safes. Some examples include personal legal documents, bank statements, identity documents and business agreements.
- NEVER photograph military personnel or facilities. Appropriate conditions may include functions outside of normal hours of operation (social settings) and when military personnel are out of uniform.
- Beware of overly friendly or overly interested individuals
- DO NOT hand-carry or transport packages for other people when traveling back to the U.S. Use appropriate and authorized delivery methods.

Activities and Behavior

- Avoid areas of unrest, demonstrations, protest or high crime locations
- If you are detained or arrested:
  - ☑Contact the local U.S. Embassy or Consulate
  - ☑Do not make any statements or sign any documents without legal consult from a U.S. Embassy or Consulate representative

Upon your Return

- Upon returning from PTO travel (multiple travel routes, visits, transits and final destination locations) you will need to have a security debrief that will include:
- Reporting all contacts with persons of any foreign nationality especially when:
  - ☑ Illegal or unauthorized access to classified or sensitive information is sought
  - ☑ Notify Security IMMEDIATELY, if you are concerned that you may be the target of an actual exploitation or attempted exploitation by a foreign entity.
- Notification to Security Personnel of any unusual incident(s) or circumstances

Emergency Notification

- Provide in advance to family or close friends; your anticipated contact information in the event of an emergency.
- Include instructions on how to contact the 24-Hour State Department Operations Center telephone number (202) 647-1512. They may be able to assist others in reaching you.
- The American Red Cross is a very helpful resource in cases of serious life-threatening medical emergencies.

GLS Security Contact Information

- **GLS PMO Security Department – Herndon:**
  - ☎ Rick Eldard – Director of Security: (703) 995-1361
  - ☎ Linda Richardson – Facility Security Officer: (703) 703-995-1384
  - ☎ Robert Wolf – Assistant Facility Security Officer: (703-995-1366

- **GLS DEPCEN Security Department – Herndon:**
  - ☎ Leon Cliette – Dep. Director of Deployment Security (703) 995-1391
  - ☎ Joshua Finch – Security Lead (703) 995-1348
  - ☎ Mohammed Shams – Security Lead (703) 995-1375

- **GLS ISMO Security Department – Baghdad**
  - ☎ Kerry Superville – Special Security Officer DSN (318) 822-5473
  - ☎ Angel Salazar – Assistant Special Security Officer

  - ☎ **US INTERNATIONAL SECURITY HOTLINES**
  - ☎ Defense Hotline (800) 424-9098
  - ☎ Central Intelligence Agency (703) 874-2600
  - ☎ Federal Bureau of Investigations (202) 324-3000
  - ☎ Nuclear Regulatory Commission (800) 233-3497
  - ☎ Department of Energy (800) 541-1625

Questions and Answers

This concludes the Defensive Travel Briefing – Thank You!

EXHIBIT 3

Global Linguist Solutions

SECURITY BRIEFING CERTIFICATE FORM
Initial Security Awareness Training

My signature below indicates that I understand and acknowledge my individual responsibility regarding the **GLS Initial Security Awareness Training**. Components include:

(1) Initial Security
(2) Operations Security/Communications Security and
(3) Defensive Travel

Employee Full Name: JAMES FRANCIS HITSELBERGER **EE ID#:** June 30, 20 2011

Site Location: Kuwait

On completion of the training complete this Security Briefing certificate attesting that:

I have completed my initial security training and understand my responsibilities to protect, preserve and safeguard GLS proprietary information and intellectual properties.

I understand I am not to remove from my assigned work area(s) any GLS proprietary information, intellectual properties, Personally Identifiable Information (PII), equipment or other materials without prior written authorization.

My access to classified information or sensitive information requires my acceptance and responsibilities associated with safeguarding sensitive information in accordance with prescribed security standards. Classified and sensitive information which I may be granted access will be used only for the purpose for which released.

I understand that a DOD Security Clearances can be suspended or revoked for violation of security regulations or improper use of classified information. I also understand I could be subject to action under the espionage statutes of Federal Law with respect to my failure to handle or deliberate mishandling of classified information; that my suitability is continually assessed and I am subject to a background investigation, subject interview, Counter-Intelligence/Force Protection Screening or Polygraph Examination at the discretion of the US Government.

I understand that upon termination of my access to classified or sensitive information, my responsibility does not end pertaining to my safeguarding of known classified information and this remains in effect until the security classification is removed by appropriate U.S. Government authority.

NOTE: Questions concerning this briefing should be directed to the GLS PMO Security Office.

James Hitselberger — June 30, 2011
Employee Acknowledgement Signature **Date**

Kenneth Spinner — 6/30/2011

Collection of this information is authorized by Executive Order 9397, 10450, 12356; U.S.A. 301 and 7531-532; 15 U.S.A. 1501 et seq; and 44 U.S.C. 3101.

ENCLOSURE (F)

EXHIBIT 4

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
[signature]	Aug-27, 2011	388-30-5649

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

Global Linguist Solutions, LLC
3190 Fairview Park Drive, Suite 1000
Falls Church, VA 22042

WITNESS	ACCEPTANCE
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.	THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.
SIGNATURE: [signature] DATE: 08/27/2011	SIGNATURE: [signature] DATE: 8/27/2011
NAME AND ADDRESS (Type or print): Anna Dupree, Program Support Manager/CRC, Global Linguist Solutions, LLC (4QZW3), 3190 Fairview Park Drive, Suite 1000, Falls Church, VA 22042, Tel (571)641-9892	NAME AND ADDRESS (Type or print): Linda K. Richardson, Facility Security Officer, Global Linguist Solutions, LLC (4QZW3), 3190 Fairview Park Drive, Suite 1000, Falls Church, VA 22042, Tel (703) 995-1384, Fax (703) 995-1378

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS
ANNA DUPREE	

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN HITSELBERGER, James Francis AND THE UNITED STATES

(Name of Individual - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

ENCLOSURE (6)

EXHIBIT 5

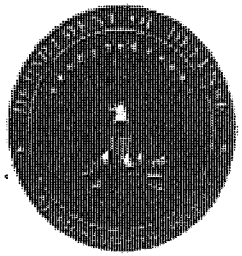
Certificate of Completion

James Hitselberger

Has completed

Information Assurance Awareness

Version 9.0, 2011



9/26/2011

Signature *Date*

paper form.

OUTINE USES: None.

ISCLOSURE: Disclosure of this information is voluntary; however failure to provide the requested information may impede, delay or prevent further processing of this request.

ART I (To be completed by Requestor)

ME:	James (FIRST)	F (MI)	Hitselberger (LAST)
. COMMAND:	JSOTF-GCC	6. CITIZENSHIP: US	7. DESIGNATION:
. BUILDING:	BANZ4	☒ US	☐ MIL RATE/RANK: ☐ ACTIVE ☐ RES
. DEPARTMENT:	J3	☐ FN CC:	☒ CIV
. PHONE:	4396164	☐ OTHER	☐ CTR PART II.15-17 REQUIRED
. NETWORK CCESS	☒ SIPRNET	☒ NIPRNET	☐ PRIVILEGED: N6/IAM/IAO Signature:

. PREVIOUS NSW COMMAND TO TRANSFER ACCOUNT(S) FROM:

0. JUSTIFICATION FOR ACCESS: - EMAIL, OFFICE SUITE TO CONDUCT WORK RELATED REQUIREMENTS

IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS

1. INITIAL	YOU AGREE TO COMPLIANCE WITH:
> JH	By initialing, you acknowledge and consent that when you access Department of Defense (DoD) information systems, you will abide by the User Agreement on reverse side of this form.
> JH	Information Assurance Training/CBT completed (If IA Training completed within last year, AND you have a copy of the IA Training certificate, please attach to this form in lieu of completing training again).
> JH	I understand I am required to complete Annual Information Assurance Training.

2. USER SIGNATURE: James Hitselberger — 13. DATE: Sept. 6, 2011

..T II – ENDORSEMENT OF ACCESS

4. VERIFICATION OF NEED TO KNOW BY SUPERVISOR certify that this user requires access as requested. ☑

ACCESS EXPIRATION DATE:

15. COMPANY:

16. CONTRACT #:

17. EXPIRATION:

8. SUPERVISOR'S NAME (Print Name – Last, First, Grade/Rank): Golczynski, Mark E7 — 19. ORG/DEPT: J3 — 20. PHONE NUMBER:

1. SUPERVISOR'S SIGNATURE — 22. EMAIL ADDRESS:

ART III – SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

3. TYPE OF INVESTIGATION: NAC — 24. DATE OF INVESTIGATION: 20110708 — 25. CLEARANCE LEVEL: INTERIM Secret

3. VERIFIED BY (Print Name – Last, First, Grade/Rank): Lacher Ray — 27. PHONE NUMBER: 439-3133 — 28. SECURITY MANAGER SIGNATURE

ART IV – COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

INFORMATION ASSURANCE MANAGER (IAM) CHECK-IN / CHECK OUT (Print Name – Last, First, Grade/Rank) — CHECK-IN SIGNATURE/DATE: NARCEL M. HERMOSILLA 8SEP2011

UNT CREATED BY: (Print Name – Last, First, Grade/Rank): VRVIN, DESMOND IT2/E-5 — DATE: 06SEP11

ENCLOSURE (B)

nformation systems:

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

You consent to the following conditions:

- The U.S. Government routinely intercepts and monitors communications on this information system for purposes cluding, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the U.S. Government may inspect and seize data stored on this information system.
- Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, ny U.S. Government actions for purposes of network administration, operation, protection, or defense, or for ommunications security. This includes all communications and data on an information system, regardless of any pplicable privilege or confidentiality. The user consents to interception/capture and seizure of ALL communications and ata for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). lowever, consent to interception/capture or seizure of communications and data is not consent to the use of privileged ommunications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any arty and does not negate any applicable privilege or confidentiality that otherwise applies.

Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of onfidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly ncouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to ely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not .cient to create such protection where none exists under established legal standards and DoD policy.

A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not aive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD olicy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such ommunication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable rivilege or confidentiality.

These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use nd disclosure of privileged information, and thus such communications and data are private and confidential. Further, ne U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged ommunications and data to ensure they are appropriately protected.

In cases when the user has consented to content searching or monitoring of communications or data for personnel isconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other han privileged communications or data that are related to personal representation or services by attorneys, sychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance /ith DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or isclosure of such information.

.ll of the above conditions apply regardless of whether the access or use of an information system includes the display f a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the onditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full etail or provide a summary of such conditions, and regardless of whether the banner expressly references this User greement.

understand that to ensure the integrity, safety and security of Naval Special Warfare IT resources, when using those urces, I SHALL:

eguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.

Protect Controlled Unclassified Information (CUI) and classified information to prevent unauthorized access,

procedures. Immediately report any suspected or confirmed compromise of any information security issue to the local Command Information Assurance Manager (IAM)/Information Assurance Officer and/or to the NSW Headquarters IAM, Ms. Telma Báez-Vaughan, (619) 437-5800 or IAO, Mr. Steve Higgins, (619) 437-5364.
Access only that data, control information, software, hardware, and firmware for which I am authorized access and have a need-to-know, and assume only those roles and privileges for which I am authorized.
subject to monitoring, and further understand that there is no expectation or right to privacy over the data and .munications generated through my use.
r-iomptly lock workstation or log off the network and appropriately secure drive as necessary when not in use.
Limit my computer use to official Government business and understand that failure to comply may result in punishment and/or NCIS investigation.
Store classified data only on properly marked removable media or a LAN system approved for storage at the sensitivity level of the classified data.
Protect and label all printed output and magnetic media in accordance with the HIGHEST level of classification of information processed on the system.

further understand that, when using NSW IT resources, I SHALL NOT:
Access commercial web-based e-mail (e.g. HOTMAIL, YAHOO, or any other email accessed by a web browser)
Auto-forward my NSW official e-mail to a commercial e-mail account.
Bypass, strain, or test IA mechanisms (e.g., Firewalls, content filters, anti-virus programs, etc.). If IA mechanisms must be bypassed, I shall coordinate the procedure and receive written approval from the Local IA Authority (IAM/IAO).
Introduce or use unauthorized software, firmware, or hardware on any NSW IT resource without written authorization from the Local IA Authority.
Access peer-to-peer sites (e.g., Limewire, Kazaa, Skype, BitTorrent, etc.)
Download copyrighted files (e.g., .mp3, .wav, .mov, .avi) to my DoD-issued government system
Relocate or change equipment or the network connectivity of equipment without written authorization from the Local IA Authority.
Use personally owned hardware, software, shareware, or public domain software without written authorization from the Local IA Authority.
Introduce or utilize personal or government issued Personal/Portable Electronic Devices (PED) wireless capable devices (e.g. cellular telephones, Smartphone, two-way pagers, PDAs, laptops) within any Naval Special Warfare (NSW) facility.
oad executable files (e.g., .exe, .com, .vbs, or .bat) onto NSW IT resources without the approval of the Local IA .hority.
Participate in or contribute to any activity resulting in a disruption or denial of service.
Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
Commit computer fraud, including unauthorized input of false records of data into the system or unauthorized alteration or destruction of information files or equipment.
Put NSW IT resources to uses that would reflect adversely on Naval Special Warfare (e.g., uses involving pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violation of statute or regulation, inappropriately handled classified information; and other uses that are incompatible with public service).

dditionally I WILL ABIDE by the SOFTWARE CODE OF ETHICS below:
All personnel shall use command software only in accordance with the license agreement stated by the developer.
The following points are to be followed in order to comply with software license agreements:

1. Legitimate software will promptly be provided to all personnel who can justify the need for such software.
2. The unauthorized use of software will not be tolerated at this command. Any personnel illegally reproducing software can be subject to civil and criminal penalties including fines and imprisonment. Illegal copying of software under any circumstances is prohibited.
3. No one shall give command software to anyone outside the command.

USER NAME (Print Name – Last, First, Grade/Rank): Fitzgerald, James Civ	
USER SIGNATURE: James Fitzgerald	DATE: Sept. 6, 2011

A. PART I: The following information is provided by the user when establishing USER ID

(1) NAME. The first name, middle initial and last name of the user.
(2) COMMAND. The command the user is assigned to.
(3) BUILDING. The building the user is assigned to.
(4) DEPARTMENT. The department code the user is assigned to (i.e. N6)
(5) PHONE. The telephone number user can assigned to user in the following format (XXX) XXX-XXXX DSN: XXX-
(6) CITIZENSHIP. Select appropriate citizenship US, FOREIGN NATIONAL, or OTHER. Enter country code if required.
(7) DESIGNATION. Select appropriate designation and enter additional information required.
(8) NETWORK ACCESS. Select appropriate network(s) request is for Privileged access requires separate appointment and user agreement
(9) PREVIOUS NSW COMMAND TO TRANSFER ACCOUNTS FROM. Enter NSW command you have just transferred from.
(10) JUSTIFICATION FOR ACCESS. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date. This information is can be customized to site specific requirements.
(11) INITIAL. User must initial by requested IA requirements indicating compliance with the associated documents, training, or certification.
(12) USER SIGNATURE. User must sign the SAAR with the understanding that they are responsible and accountable for their password and access to the system(s).
(13) DATE. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(14) VERIFICATION OF NEED TO KNOW BY SUPERVISOR. To verify that the user requires access as requested.

CESS EXPIRATION DATE. The user must specify required ...rmation if user is a contractor OR IF ACCESS IS REQUIRED FOR ...ESS THAN 1 YEAR.

(15) COMPANY. If user is a contractor indicate company user's employer
(16) CONTRACT #. If user is a contractor indicate the contract number.
(17) EXPIRATION. If user is a contractor indicate expiration date of contract ELSE if access is required for less than 1 year indicate date access must expire.
(18) SUPERVISOR'S NAME. The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
(19) ORG/DEPT. Supervisor's organization or department.
(20) PHONE NUMBER. The Supervisor's telephone number in the following format (XXX) XXX-XXXX DSN: XXX-
(21) SUPERVISOR'S SIGNATURE. Supervisor's signature is required by the endorser or his/her representative.
(22) EMAIL ADDRESS. Supervisor's email address.

C. PART III: Certification of Background Investigation or Clearance.

(23) TYPE OF INVESTIGATION. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).
(24) DATE OF INVESTIGATION. Date of last investigation.
(25) CLEARANCE LEVEL. The user's current security clearance level (Secret or Top Secret).
(26) VERIFIED BY. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.
(27) PHONE NUMBER. The Security Manager's telephone number in ... following format (XXX) XXX-XXXX DSN: XXX-
(28) SECURITY MANAGER SIGNATURE. The Security Manager or ...s/her representative indicates that the above clearance and investigation information has been verified.

D. PART IV: This information is site specific and can be customized

HELPDESK CHECK-IN/CHECK-OUT.

HELPDESK CHECK-IN SIGNATURE/DATE. Indicates that User has properly checked-in with the HelpDesk and the Technician that signs has given the User guidance regarding steps to take to obtain account and directed User to additional check-in POCs.

HELPDESK CHECK-OUT SIGNATURE/DATE
Indicates that User has properly checked-out with the HelpDesk and the Technician that signs has ensured that all equipment assigned to the user is returned and updated within the CMDB.

COMMON ACCESS CARD (CAC) CHECK-IN / CHECK-OUT

COMMON ACCESS CARD (CAC) CHECK-IN.
Indicates that User has properly checked-in to schedule date/time for registration of CAC with POC.

COMMON ACCESS CARD (CAC) CHECK-OUT.
Indicates that User has properly checked-out with POC and is informed that User will be required to return to a CAC Issuance Office to either return or update signatures on CAC.

INFORMATION ASSURANCE MANAGER (IAM) CHECK-IN / CHECK-OUT.

INFORMATION ASSURANCE MANAGER (IAM) CHECK-IN.
Indicates that User has properly checked-in with IAM and has been briefed appropriately by POC.

INFORMATION ASSURANCE MANAGER (IAM) CHECK-OUT. Indicates that User has properly checked-in with IAM and has been debriefed appropriately by POC.

E. PART V: USER AGREEMENT REQUIRED. Sites may modify IAM/IAO information and add additional site specific information.

F. DISPOSITION OF FORM:
TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.
FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO Recommend file be maintained by IAO adding the user to the system.

SUBMIT COMPLETED SAAR FORM AND USER AGREEMENT TO HELPDESK ALONG WITH COPY OF THE FRONT OF CAC CARD and IA TRAINING Certificate.

ENCLOSURE (2)

	Signature	Command	UTC	
CAPT TINSLEY		U3	39966	
LCDR WITT		U3	39966	
SOCM BOWES				
SBCM PUERSTENBERG		GCC		
CDR ROULSTON		GCC		
PSC JOHNSON		U3	39966	
YNC JENKINS		U3		
YNC GAUSE		JSOTF-GCC		
YN2 FLORES				
YN1 CRISS		U3	39966	
SrA WALELA		JSOTF-GCC		
SrA SAN MARTIN				
LCDR BOLDEN		U-3	3.9934	
LTJG BROWN		GCC		
ISC WATSON		U-3	39966	
IS1 JOSE		NSWU-3	39966	
IS2 NOWAK		U3	39966	
IS1 ECHEVERRIA		JSOTF-GCC		
IS2 YOUNG		U3	39966	
LCDR ELLIS		U3	39966	
LCDR LOZADA		U3	39966	
SgtMaj ANDERSON				
CPT THIEL				
MSG CHRISTENSEN		JSOTF		
LT BENEVENTO		U3	39966	
LT HERRON				
CWO3 DESTEFANO		U3	39966	
SSGT SYVERSON				
SOCS NEBEL		U3		
SOC DEWALT				
EOC GREEN				
SOC DENNY				

ITC ~~SSgt~~ MATHIS		JSOTF - GCC		
IT2 LEWIS, D.				
IT2 ARAGON		JSOTF - GCC		
~~TRANS - SSgt RODOLOSI~~	TRANSFERRED			
ET1 BURRHUS				
SSgt ALMEIDA		JSOTF-GCC		
SSgt LeBLANC		JSOTF-GCC		
IT2 HARTE		JSOTF-GCC		
ET2 ~~ET2~~ BUR		NSWU-3		
SrA WHITE				
IT2 LEWIS, E		NSWU-3		
IT2 IRVIN				
IT1 JEDLICK		NSWU-3	59966	
~~SrA JOHNSON~~	TRANSFERRED			
~~TRANS - SrA VALLEE~~	TRANSFERRED			
IT2 ANDRADETORRES		JSOTF-GCC		
~~TRANS - SSgt~~ VORLANDER	TRANSFERRED			
~~TRANS - SSgt WELLS~~	TRANSFERRED			
SSgt VERGARA		JSOTF - GCC		
IT2 KEMPF		JSOTF - GCC JD		
SSgt HARRY		JSOTF GCC / JD		
TSgt KREKOW		JSOTF-GCC / JD		
ET2 ~~IT2~~ ASHBURY		NSWU3		
IT2 SOUTH				
SrA BARRETT				
TSgt DORRIS		JSOTF - GCC JD		
SrA LAING		JSOTF - GCC JD		
IT2 SMITH		NSWU-3	59966	
IT2 SANDEEN		NSWU-3	59966	
[redacted]				
CWO3 FROST		NSWU3	59966	
GMC SHIPMON		NSWU-3	59966	
GM1 CALDWELL				
GM1 DESPOPOULOS	LV LEAVE			
GM1 BROWN		JSOTF GCC / REVIEW		
AO1 RED	TAD			
GM1 CLOUSE	TAD			
GM2 BENEDICT	TAD			
TSGT HURT	TAD			
GM2 MCVANN	TAD			

SBC FREDRICH	TAD			
ND1 FROST	TAD			
SOC MCBURNETT	TAD			
SBC MCREA				
BM1 PRICE				
FC1 CRAMER	WATCH			
OS1 FRAISER		JSOTF-GCC		
NDC PARKER	TAD			
FR1 GULICK		NSWU-3		
QM1 STEMBRIDGE	LEAVE			
ND2 DAVIS		NSWU-3		
OS2 TYSON	TRAVEL			
SO1 LEASURE	TAD			
SOC COLLINS	TAD			
SFC JONES	TRAVEL			
SO1 SCOTT				
SOC CASSIDY	TAD			
NDCS PHANTHAVONG				
SBC BUOB				
LCDR EGGE		USN	39966	
MAJ WOOD	TAD			
LT DISHER				
LTJG HULSE				
SMSgt SYMES-CREARY		JSOTF-GCC		
LSC NEGRON		USN		
LS1 MULANAX		USN		
LSC JOHNSON		USN		
LS1 DAVIS	TDA			
LS1 DUCK		JSOTF-GCC		
ABF2 BURMAHL		JSOTF-GCC		
LS2 PILIGAN		N4/N3		
BUC BRYAN		USN		
EO1 ACUTIM		N4/N3	39966	
CM2 STEFFEY		USN		
SSgt ESPIRITU		JSOTF-GCC		
CW04 HERMOSURA		NSWU-3	39966	
1ST LT LEATHERBURY		JSOTF-GCC		
ITC LYLES				

GM2 GIBBONS				
LCDR HOLDER		GCC	39966	
HMC JUAN		U3	39966	
HM FARRELL		U3	39966	
HORSTING		GCC		
MSgt POINSETTE		GCC		
MSgt WILLIAMSON		GCC		
LAWANDA WASHINGTON				
SSgt SMITH				

NI

CW03 Sarmiento

YN1 Solomon

LACHE RAY

SOCM BAGGETT, NICKY

GM(SW) MIKE REHFUSS

Gandul Gandul

James Hitselberger

Otto AMON

Ken Figueras

JACK Black

KATHLEEN KNIGHT J8

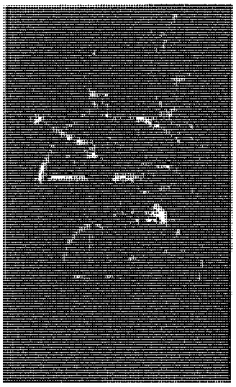
Itziar Igartua-Vazquez J4

Randy Shoulders J4

LT SG CALDWELL

LT JG GATLEY

EXHIBIT 6

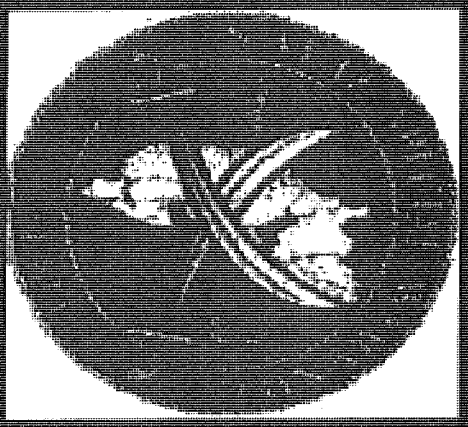


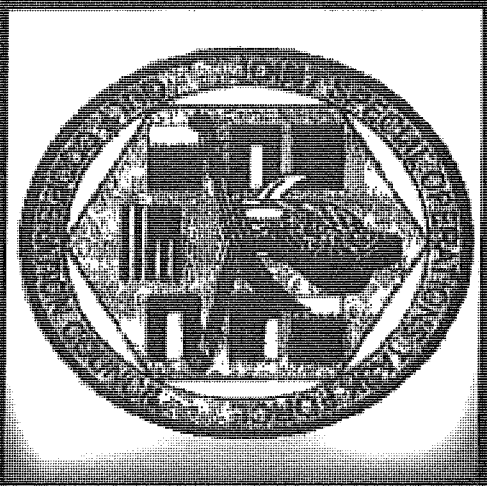
AWARDEES BRIEF

SECURITY

2011

AWARDEES BRIEF





ENCLOSURE (D)

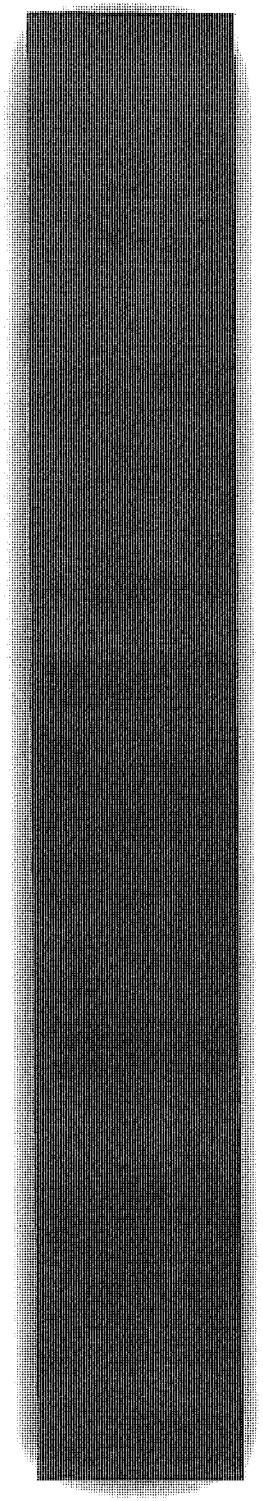
SECURITY MESSAGE

The protection of Government assets, people and property, both classified and controlled unclassified, is the responsibility of each and every member of the Department of Defense, 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. Anything less is simply not acceptable. This Initial Security Indoctrination provides a good foundation. Your Agency/Department will supplement this indoctrination with local security policies, procedures, and responsibilities.

CONTENTS

- Physical Security
- Information Security
- Personnel Security
- Security Violations



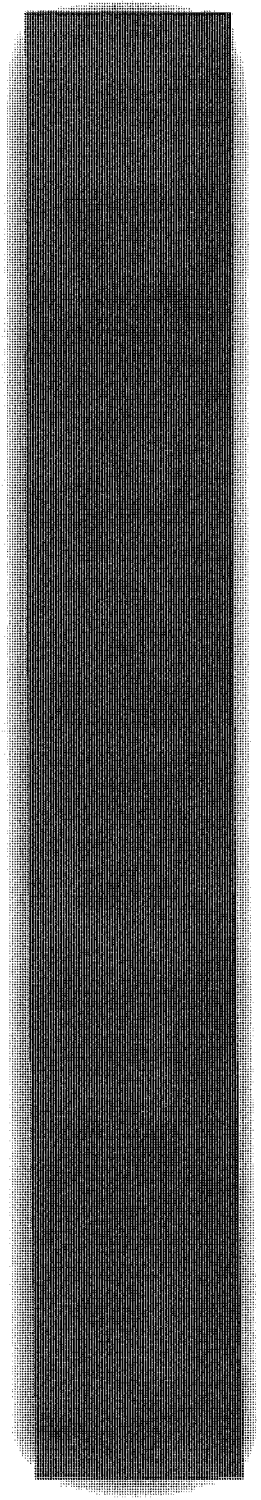
WHY SECURITY?

- DoD Security Regulations, Directives, and Programs are established to counter threats
- Threats to classified and unclassified government assets can include:
  - Insider (government employees, contractor employees, and authorized visitors)
  - Criminal and Terrorist Activities
  - Foreign Intelligence Services
  - Foreign Governments

PHYSICAL SECURITY

Physical security offers security-in-depth, and includes, but is not limited to:

- Perimeter fences
- Employee and visitor access controls
- Badges/Common Access Cards (CAC)
- Intrusion Detection Systems (IDS)
- Random guard patrols
- Prohibited item controls
- Entry/exit inspections
- Escorting
- Closed circuit video monitoring



INFORMATION SECURITY

- Pertains to the protection of classified and sensitive information, to include but not limited to:

Marking
- Transmission
- Destruction

Handling
Storage

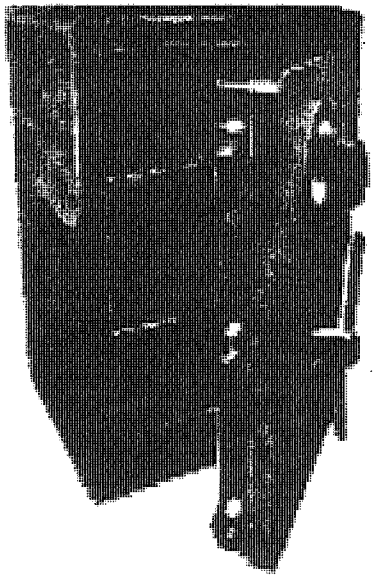
INFORMATION ASSURANCE

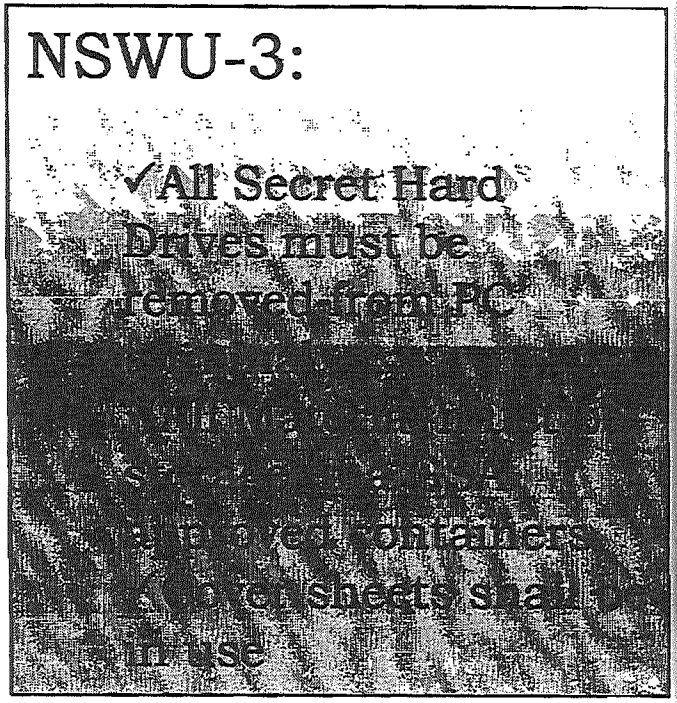
- In the performance of your duties you may be required to have access to government computer systems.

- Information assurance protects and defends information and information systems by ensuring their availability, integrity, authenticity, confidentiality

Additional information is available from the Information Assurance Manager: Mr. Kenneth Figueras

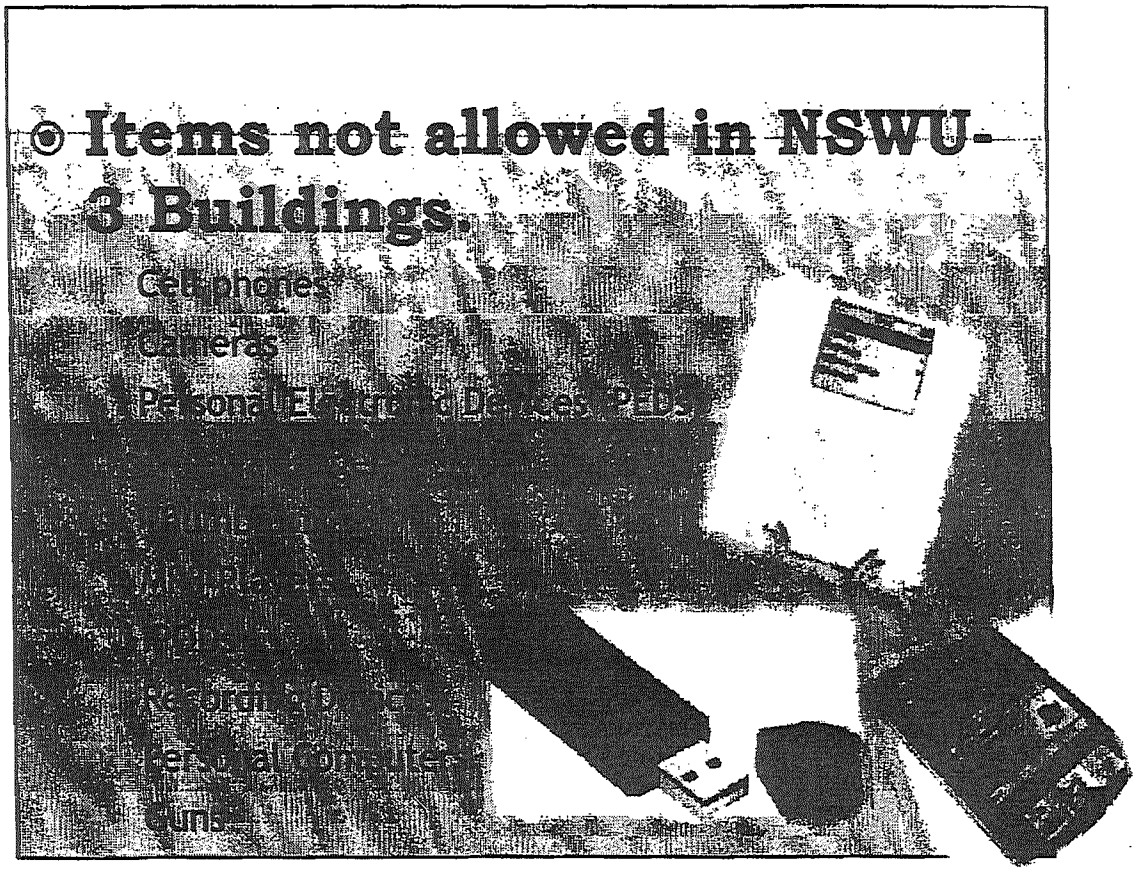
STORAGE REQUIREMENTS





PROHIBITED ITEMS

- **Items not allowed in NSWU-3 Buildings.**
  - Cell phones
  - Cameras
  - Personal Electronic Devices (PEDs)
  - [illegible]
  - [illegible]
  - [illegible]
  - Recording Equipment
  - Personal Computers
  - Guns



- These Items should be left in your vehicle
  - [illegible]
  - Boxes.

CLASSIFICATION LEVELS

There are *THREE* levels of Classification

TOP SECRET

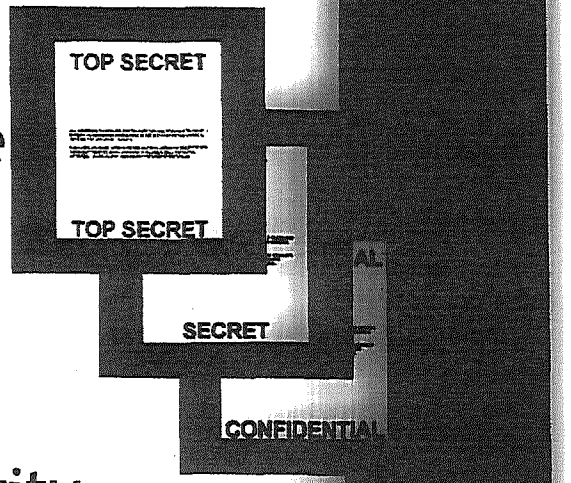
Exceptionally Grave Damage to the National Security

SECRET

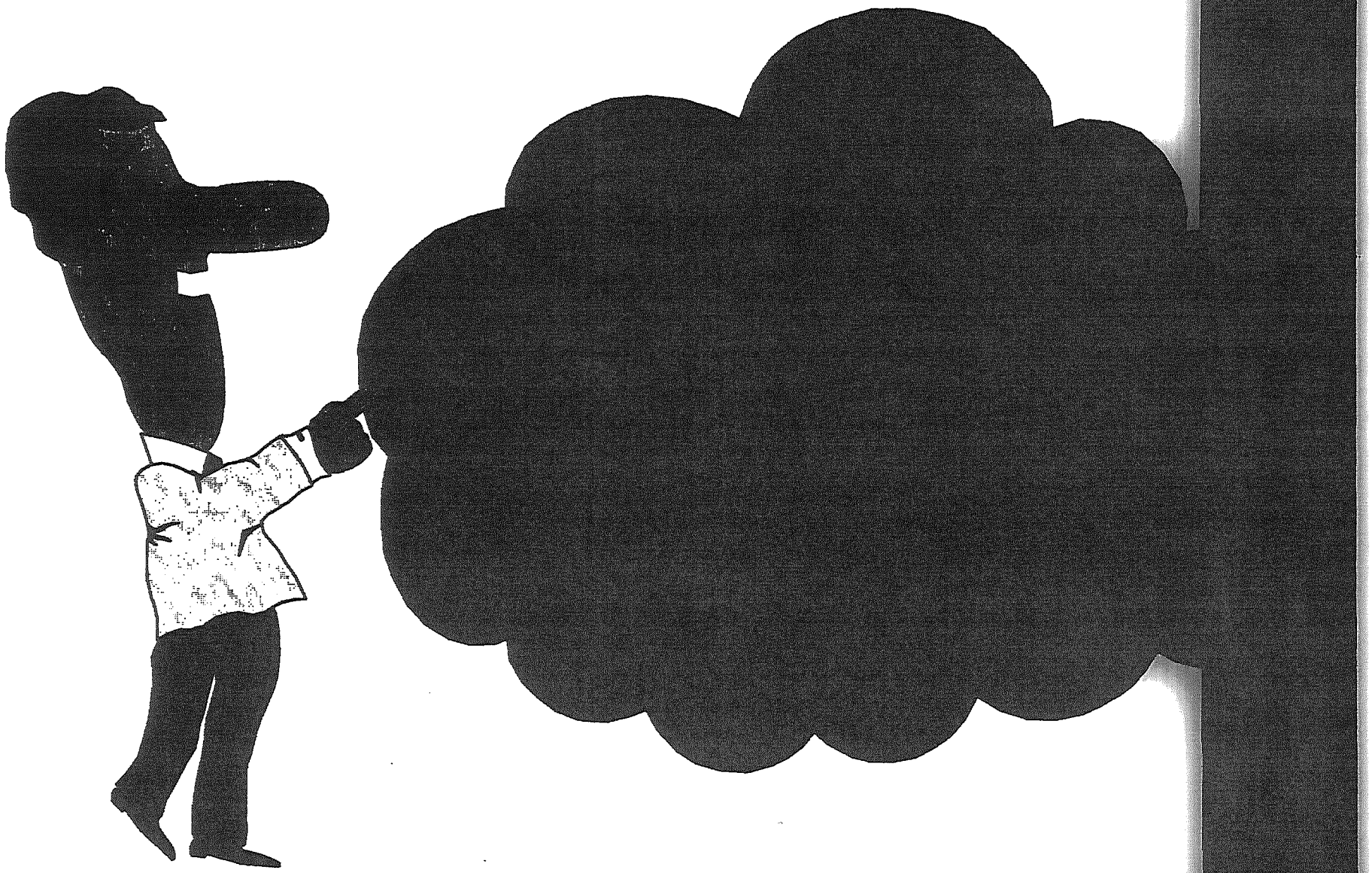
Serious Damage to the National Security

CONFIDENTIAL

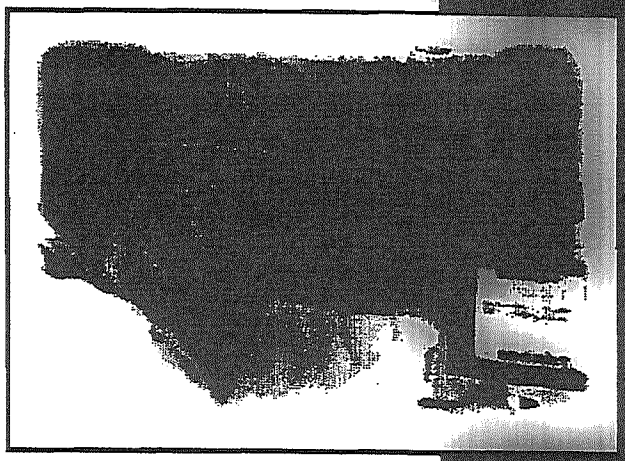
Damage to the National Security



Classified Material can include ANY of these and must be properly marked:



CLASSIFIED INFORMATION



- Must be under the control or guarded by an authorized person or stored in a locked security container, vault, room, or secure area
- Must be discussed on secure telephones or sent via secure communications
- Must be processed on approved equipment
- Must be destroyed by approved methods
- Must be discussed in an area authorized for classified discussion.

PERSONNEL SECURITY

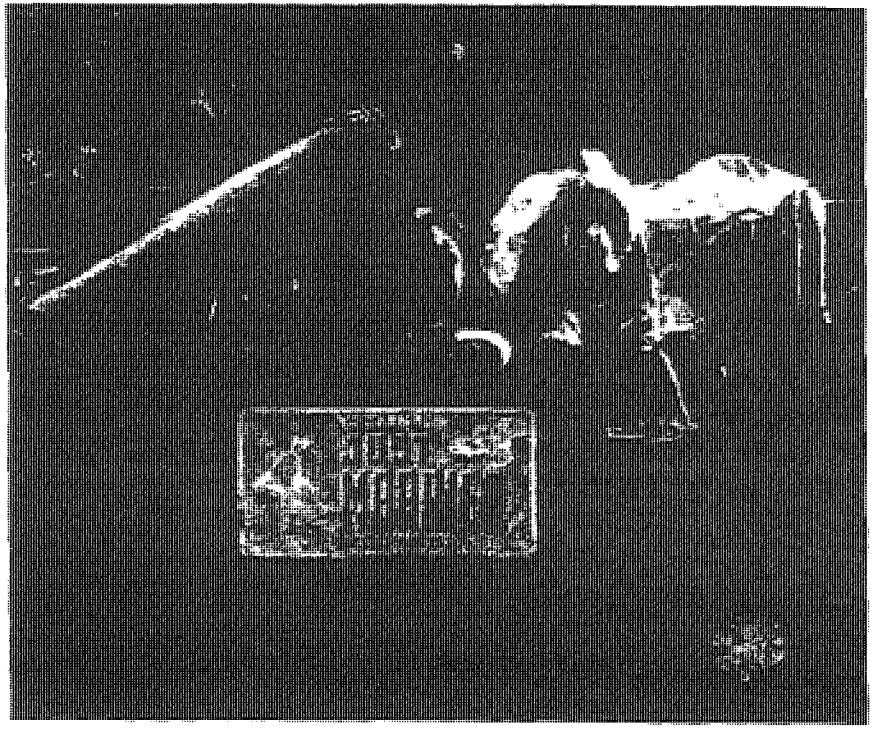
- Your position sensitivity and/or duties will determine your level of security clearance or access

- There are three levels of security clearance:
  - Top Secret
  - Secret
  - Confidential

- **Note: SCI is an access program, NOT a clearance. But it's a very important access to maintain, if needed. For SCI access please contact Ms. Laché Ray, NSWU-3 SSO.**

REPORTING REQUIREMENTS...

- You Must Report Change of:

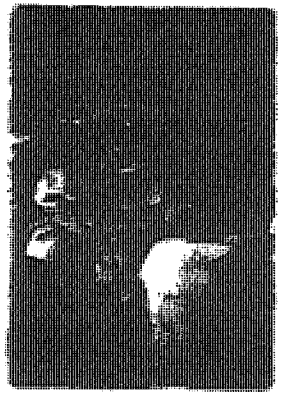


Name

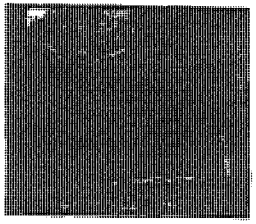
Marital Status

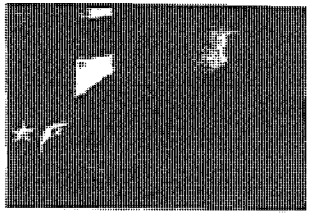
Citizenship

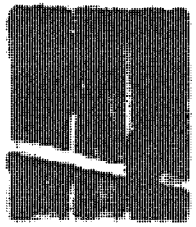
YOU MUST REPORT...

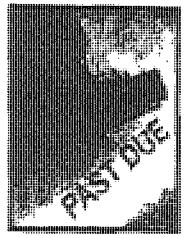


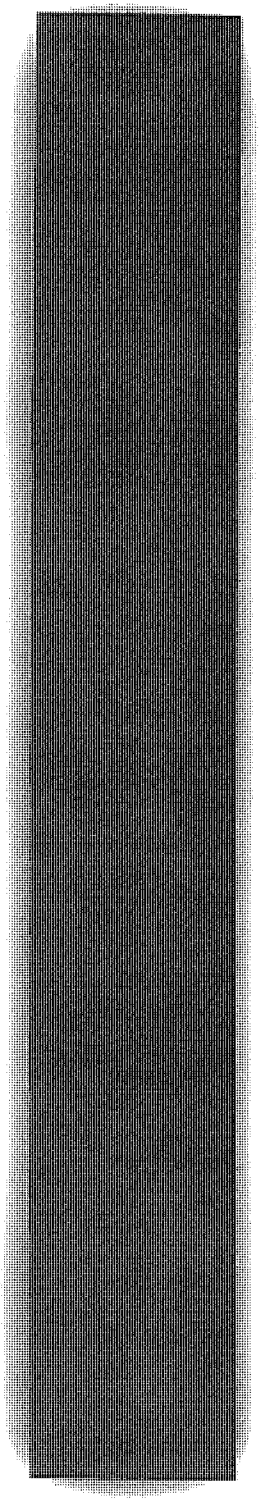
- Adverse information concerning yourself or a co-worker.
- Adverse information includes, but is not limited to recent arrests, alcohol or drug related problems, and/or financial difficulties.
- Loss, compromise, (or suspected loss or compromise) of classified information, including evidence of tampering with a security container used for storage of classified information.
- All continuing contacts with foreign nationals, to include shared living quarters and marriage.
- Suspicious contacts with/by foreign nationals





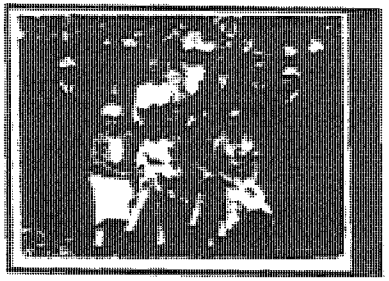


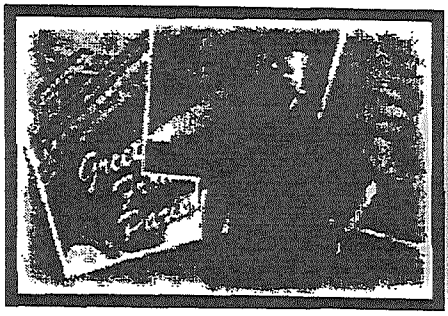




YOU MUST REPORT...

- If a member of your immediate family (or your spouse's immediate family) is a citizen or resident of a foreign country.
- Married to a Foreign National or Intent to marry a Foreign National.
- 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.
- Foreign travel in accordance with your agency's policies and procedures.
- All holders of a security clearance must report information to their security office that might have a bearing on their continued eligibility for access to classified information.





SECURITY VIOLATIONS

A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, whether or not a compromise results. No matter how minor, any security infraction must be reported immediately to the security office so that the incident may be evaluated and any appropriate action taken.

The following are some examples of security violations:

- Leaving a classified file or security container unlocked and unattended either during or after normal working hours.
- Bringing your cell phone into any NSW buildings.
- Keeping classified material in a desk or unauthorized cabinet, container, or area.
- Leaving classified material unsecured or unattended on desks, tables, cabinets, or elsewhere in an unsecured area, either during or after normal working hours.
- Reproducing or transmitting classified material without proper authorization.
- Removing classified material from the work area in order to work on it at home.
- Granting a visitor, contractor, employee or any other person access to classified information without verifying both the individual's clearance level and need-to-know.
- Discussing classified information over the telephone, other than a phone approved for classified discussion.

SECURITY VIOLATIONS

The significance of a security violation does not depend upon whether information was actually compromised. It depends upon the intentions and attitudes of the individual who committed the violation.

- Ability and willingness to follow the rules for protection of classified information is a prerequisite for maintaining your security clearance. Although accidental and infrequent minor violations are to be expected, deliberate or repeated failure to follow the rules is definitely not. It may be a symptom of underlying attitudes, emotional, or personality problems that are a serious security concern.
- The following behaviors are of particular concern and may affect your security clearance:
- A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline.
- Taking classified information home, ostensibly to work on it at home, or carrying it while in a travel status without proper authorization.
- Prying into projects or activities for which the person does not have (or no longer has) a need to know. This includes requests for classified publications from reference libraries without a valid need to know, or any attempt to gain unauthorized access to computer systems, information, or data bases.
- Intoxication while carrying classified materials or that causes one to speak inappropriately about classified matters or to unauthorized persons.

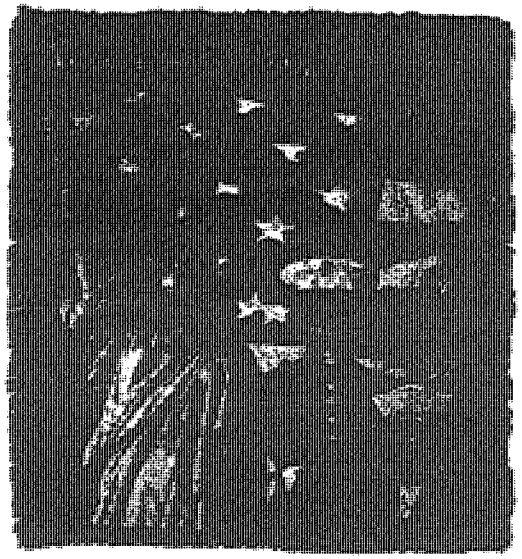
ANTITERRORISM /FORCE PROTECTION

- 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

Additional information is available from ISC Watson

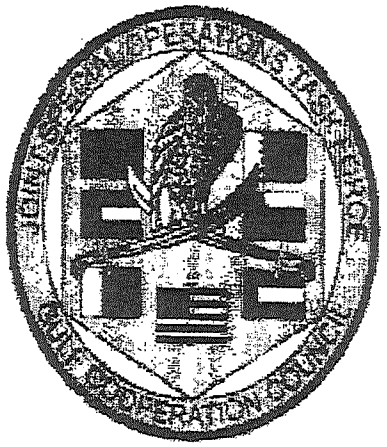
YOU CAN MAKE A DIFFERENCE!

- 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 warfighters, colleagues, and families from potential harm.



NSWU-3/JSOTF-GCC SECURITY REPRESENTATIVES

- LCDR Witt, NSWU3, Security Manager
- Ms. Laché Ray, SSO
- 1LT Leatherbury, JSOTF-GCC, Security Manager
- ENS Knight, NSWU-3, Assistant Security Manager
- YNC Gause, JSOTF-GCC, Alt Security Manager/SSR
- YN1 Criss, NSWU-3, Alt Security Manager
- IS2 Young, NSWU-3, Special Security Representative (SSR)



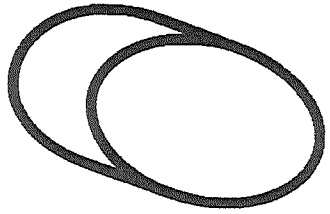
OPSEC OVERVIEW

Naval Special Warfare Unit THREE
LCDR Lozada, OPSEC Officer
IS2 Young, Asst OPSEC Officer

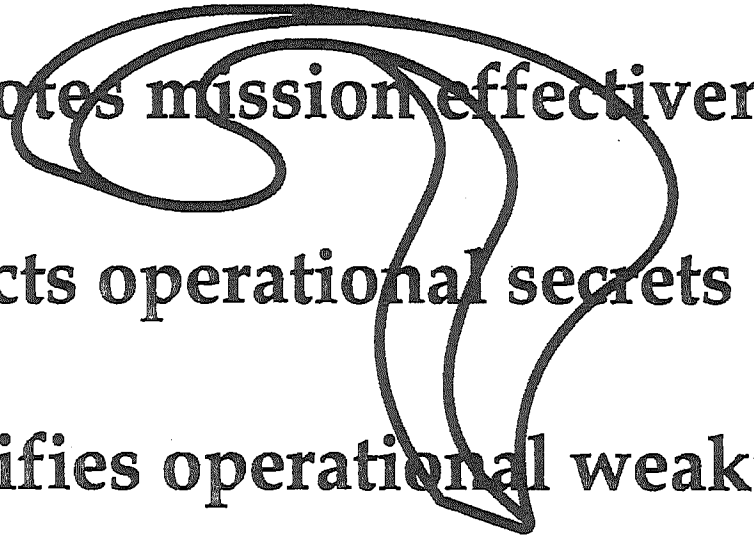
UNCLASSIFIED//FOUO

What is OPSEC?

An analytic *process* by which an organization can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.



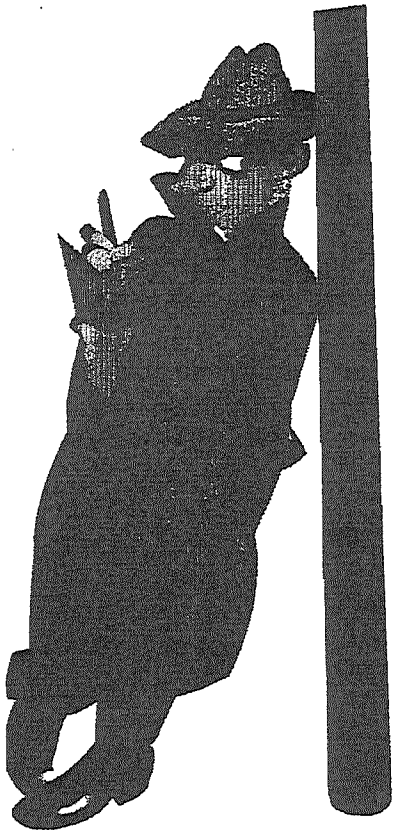
Why OPSEC?



- **Promotes mission effectiveness**
- **Protects operational secrets**
- **Identifies operational weaknesses**
- **Promotes cost-effective countermeasures**

Goal of OPSEC

- **If the adversary can't figure out what we are doing, then he will have a harder time defeating us.**

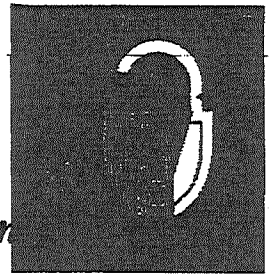


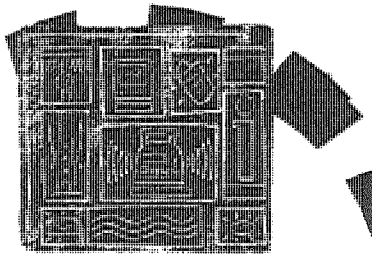
OPSEC Process

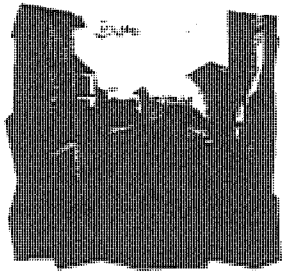
Identify
Critical Information

Analyze the
Threat

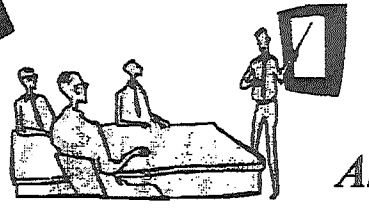
Apply Counterm







Assess Risk



Analyze
Vulnerabilities

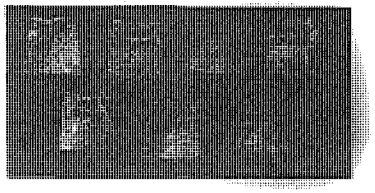
Adversary

An adversary is anyone who contends with, opposes or acts against your interest and must be denied critical information. It could be as simple and obvious as your opponent in any game, or as complex and unknown as a spy, agent of a foreign government, or a criminal.

Types of adversaries include:

- International Terrorists Groups, Criminals
- Organized Crime and Drug Trafficking Groups
- Domestic Militia Groups
- Extremists Groups and Cults
- Foreign Intelligence Agencies
- Hackers and Crackers
- Insider

Critical Information



1. Critical Information is essential to the success of an operation, mission
   or project.
2. Our Critical Information is what the Adversary needs to defeat us.

You need to think about what is critical to the adversary, not just to your organization.

Critical information includes specific facts about friendly intentions, capabilities, operations, and other activities vitally needed by adversaries for them to plan and act effectively, so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

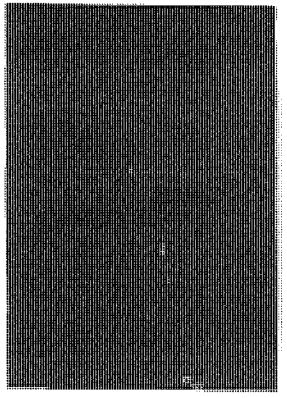
Vulnerability

A vulnerability is a weakness that can be exploited by an adversary to obtain your critical information, and it can be present in any facet of your operations.

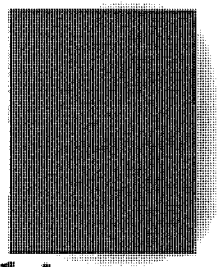
A vulnerability is weakness that can be exploited by an adversary if it is discovered. A vulnerability exists when critical information is susceptible to exploitation by an adversary.

Categories of Vulnerabilities:

- **Communications**
- **Public Affairs Department**
- **Critiques and after action reports**
- **Mail**
- **Trash**
- **E-mail**
- **Piggy-backing**



Threat



Threat is the capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of friendly activities or operations.

Who is a threat?

Any individual, organization, or country that has the intent and technical capability to attack us by exploiting our vulnerabilities.

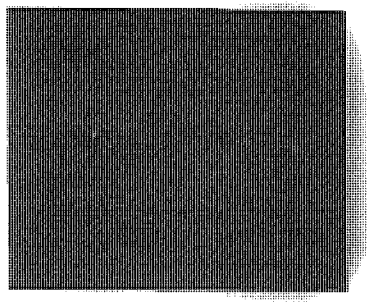
Both intent and capability must exist for the threat to exist.

Ask these questions: Does the adversary want to harm me? If yes, does he have the ability to do it?

Indicators

Indicators are observable or detectable activities or information that can be pieced together to reveal sensitive information regarding your operation. They act as clues to an activity that adversaries can exploit to their advantage through analysis.

Indicators are observable or detectable activity that may reveal information concerning an operation you are planning or about to execute. They can point to vulnerabilities. Indicators tip off the bad guys what we plan to do.



Examples:

- Special Operations Teams Deploying
- Unscheduled transfers or movements
- Large Assemblies of personnel
- Increased use of secure communications (encryption)
- Large or Frequent Meetings
- Deployment of Special Equipment
- Increased Activity in Particular Areas

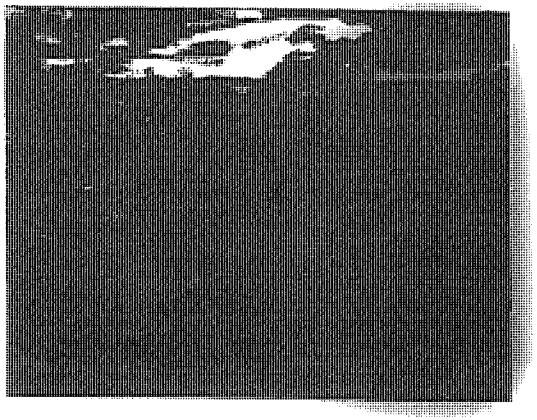
Countermeasure

A countermeasure is *anything* that effectively negates or reduces an adversary's ability to exploit our vulnerabilities.

It is whatever works! Countermeasures are used to reduce the risk to an acceptable level.

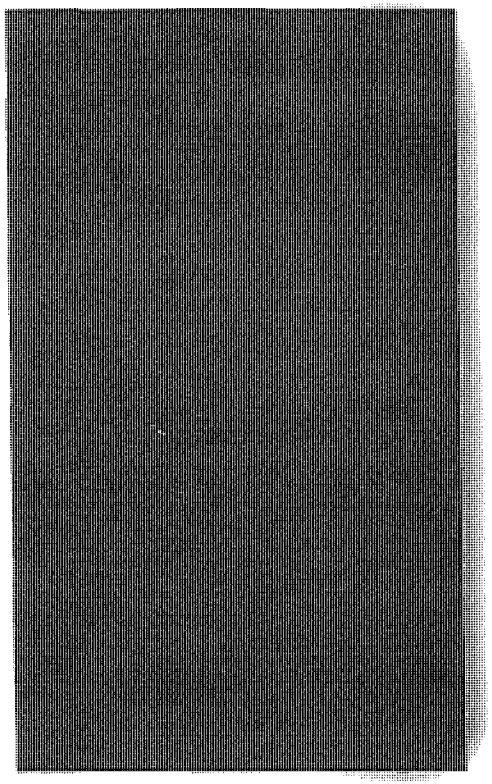
Examples of Countermeasures

- **Change your routine - route of travel**
- **Arrive and depart at unpredictable times**
- **Use lower risk methods of communications**
- **Arrive and depart at different entrances**
- **Use unmarked non-attributable vehicles**
- **Don't wear uniforms or special identifiers**
- **Use encryption**
- **Training**

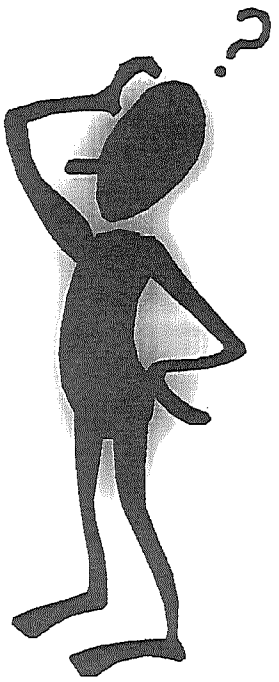


When to use OPSEC

- ALWAYS
- Special Operations Mission Planning
- Planning for Special Events
- Special Operations Training Exercises
- Plans and Standard Operating Procedures
- ALWAYS



QUESTIONS



STATEMENT OF UNDERSTANDING

You are hereby informed and made fully aware of the DOD and COMNAVSPECWARCOM policy concerning the use of USB storage devices on government computers. The policy was imposed November 2008. The use of ANY USB storage device on DOD computers (including government laptops used for travel) are strictly PROHIBITED. You are NOT to plug in any devices such as i.e. thumb drives, memory stick, Ipod, cell phone, GPS device, external hard drive (except for those approved through Change Request), XBOX, Playstation or any other devices not here mentioned with a USB connection into your computer or laptop. If you are logged in, you are responsible for that computer. If someone besides you plugs in an unauthorized device, your account will be locked out.

Penalties for plugging in an unauthorized device are:

- Member faces NJP for violation of Article 92 with relation to using a USB device on a government computer.
- Illegal device used will be confiscated by N6 Department
- Immediate account lockout (for up to two weeks)
- Member must redo User Agreement, which includes supervisor's signature.
- User must complete four Computer Based Information Assurance Training courses found at bottom of NIPRNET NSW Default home page, NKO, or AKO
- Multiple violations could result in permanent loss of computer access privileges

X James Hitselberger

Print NAME

X

User Signature

ENCLOSURE (F)

EXHIBIT 7

SECRET//NOFORN

JSOTF-GCC/NSWU-3
SITREP

1. (U) JSOTF-GCC/NSWU-3

2. (U) SITREP 104 as of 102100z APR 12, Period Covered: 092101z APR 12 to 102100z APR 12

3. (U) NSA, Bahrain

4. (S//NF)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6. (S) [redacted]

7. (S) [redacted]

EXHIBIT 8

NAVCENT N2 Regional Analysis

09 April 2012

Bahrain Situation Update

(New/modified entries in RED below)

COMUSNAVCENT produces the Bahrain situation update once a day at 0900Z.
SPOT Reports will be issued as conditions warrant.

(U) Executive Summary:

- (U) Shi'a youth conducted an illegal violent protest in Ma'ameer and Sitra, 08 APR 12. An undetermined number Ministry of the Interior (MoI) Security Forces were reportedly injured. No arrests were reported.
- (U) Shi'a youth have modified fire extinguishers to act as a compressed air gun with the ability to shoot iron rebar. This newly improvised weapon injured an undetermined number of MoI Security personnel in Ma'ameer and Sitra on 08 APR 12.
- (U) Shi'a youth attacked the Isa Town Boys Intermediate School with Molotov cocktails, 08 APR 12. No substantial damage, injuries, or arrests were reported.
- (U) The Government of Bahrain (GoB) refused to comply with a diplomatic request from the Government of Denmark seeking the extradition of jailed activist Abdal Al Hadi Al Khawajah.
- (U) The Bahraini Secretary for Nationality, Passports, and Residence Affairs announced all Bahrainis holding dual citizenship may have their Bahraini citizenship revoked if they commit an act which jeopardizes national security and/or seek legal protection under their alternate citizenship.
- (U) Expected activity: Al-Wefaq intends to hold a multiple sit-in protest in A'Ali, Bilad Al Qadeem, Al Dair, and Hamad Town at 1600C, 10 APR 12. Additional small-scale demonstration activity may occur in traditional protest areas.
- (U//FOUO) There continues to be no known specific or credible threats to U.S./Coalition forces or bases.

(U) Current Developments:

- (U) Shi'a youth conducted illegal violent protests in Ma'ameer and Sitra, 08 APR 12. The youth were reportedly protesting the death of Khadija Mohammad Ali, a 49 year-old Shi'a female who allegedly died due to complication from tear-gas inhalation. During the encounter, Shi'a youth deployed a modified fire extinguisher which acts as compressed air gun with the capability to fire rebar in the general direction when pointed. An undetermined number of MoI Security personnel were reportedly injured during the clashes in Ma'ameer and Sitra on 08 APR 12 by this new improvised weapon. The MoI responded by disbursing protesters with tear-gas. No arrests were reported.
- (U) Shi'a youth attacked the Isa Town Boys Intermediate School with Molotov cocktails, 08 APR 12. This is the 56th reported attack against a Bahraini Public School since the

NAVCENT N2 Regional Analysis

beginning of the school year, 04 SEP 11. No substantial damage, injuries or arrests were reported.

- (U) The GoB refused to comply with a diplomatic request from the Government of Denmark seeking the extradition of jailed activist Abdal Al Hadi Al Khawajah to Copenhagen for humanitarian reasons. Mr. Al Khawajah holds duel Bahraini-Danish citizenship. The Bahraini Supreme Judiciary Council stated that Mr. Al Khawajah's criminal case does not/not meet the required applicable conditions for extradition to a foreign country as stipulated by international law or preexisting bilateral agreement.
- (U) The Secretary for Nationality, Passports, and Residence Affairs announced all Bahrainis holding dual citizenship must report their alternate citizenship to the Nationality, Passports and Residency Directorate immediately according to Article 9 of the Bahraini naturalization law. Under Article 9, King Hamad reserves the right to withdraw Bahraini citizenship from any subject if they voluntarily acquired another nationality. This announcement was made after the Minister of the Interior encountered repeated cases of Bahrainis taking advantage of their duel-citizenship status by seeking protection from prosecution by invoking their alternate nationality after committing acts that jeopardized national security.
- (U) Expected activity: Al-Wefaq intends to hold a sit-in protest in A'Ali, Bilad Al Qadeem, Al Dair, and Hamad Town at 1600C, 10 APR 12. Additional small-scale demonstration activity may occur in traditional protest areas.

(U) Assessments:

- (S//REL) [redacted]
- (C//REL) [redacted]
- (U//FOUO) There continues to be no direct threat noted to US or Western interests in Bahrain. The greatest threat to US or Western personnel is collateral damage or unintended consequences from protestor or security forces activity.

(U) Unknowns:

NAVCENT N2 Regional Analysis

- (S//REL) [redacted]
- (S//REL) [redacted]
- (S//REL) [redacted]
- (S//REL) [redacted]
- (S//REL) [redacted]

(U) Current Measures:

- (U//FOUO) FPCON BRAVO plus additional measures.
- (U) The Ghuraifa area of Juffair, to the north of the Department of Defense Dependents' School and to the west of the area known as "American Alley" has been placed off-limits from 2000C – 0400C until further notice. Essential travel along Juffair Avenue, the southern boundary of this area, is authorized during those hours.
- (U) No foot or bicycle traffic is permitted between Mina Salman pier and Naval Support Activity Bahrain; only liberty busses will be used by Sailors from visiting ships.
- (U//FOUO) AMEMBASSY Manama Warden Message advises all Americans to avoid demonstrations and certain geographic areas identified on the AMEMBASSY Manama website until further notice.
    - (U) AMEMBASSY Manama updated their current force protection posture, Saar Ave. and Ave 35 have been placed off-limits to AMEMBASSY Manama employees and their dependents from 2000C – 0400C until further notice. Essential travel along these roads is authorized outside of the times indicated above.
    - (U) On 23 JAN 2012 the Department of State updated its Travel Alert for Bahrain to inform U.S. travelers of current conditions; the advisory will expire 19 APR 2012. The Alert notes that spontaneous demonstrations could turn violent with little to no notice. The alert adds that unrest is commonplace in certain neighborhoods, especially during weekends and after dark.

(U//FOUO) Demonstration notices may be found on the AMEMBASSY Manama website

Prepared by: LCDR Lawrence Cadena, COMUSNAVCENT N2, Regional Analysis Division Chief, DSN: 318-439-3631, NSTS: 998-3587.

EXHIBIT 9

Command Authorization for Search and Seizure

UNITED STATES OF AMERICA
VS.
Mr. James Francis Hitselberger

TO: Special Agent in Charge, NCIS, Middle East Field Office, Bahrain.

Affidavit(s) having been made before me by NCIS Special Agent Raffi KESICI

That there is reason to believe that on the person of and/or on the premises known as:
Navy gateway Inn and Suites, Building S317B, room 317B

which is/are under my jurisdiction,

there is now being concealed certain property, namely:
Classified information to include hard copy documents, electronic/digital computer storage media, data files, to include text and graphical image files, contained on the digital storage media attached to and/ or accompanying seizure equipment (such as but not limited to computer or other devices) for investigative purposes

I am satisfied that there is probable cause to believe that the property so described is being concealed on the person and/or premises above described and that grounds for application for issuance of a command authorized search exist as stated in the supporting affidavit(s).

YOU ARE HEREBY AUTHORIZED TO SEARCH the person and/or place named for the property specified and if the property is found there to seize it, leaving a copy of this authorization and receipt for the property taken. You will provide a signed receipt to this command, containing a full description of every item seized.

Any assistance desired in conducting this search will be furnished by this command.

Dated this 11TH day of APRIL, 2012

C S Walsh
Signature of Person Authorizing Search

CAPT USN COMMANDING OFFICER
Rank, Service, Title

NSA BAHRAIN
Command

AFFIDAVIT IN SUPPORT OF SEARCH AND SEARCH AUTHORIZATION

1. Your Affiant, Special Agent Raffi Kesici, US Naval Criminal Investigative Service (NCIS) graduated from the US federal Law Enforcement Training Center (FLETC) as a Federal Criminal Investigator, consequently completed NCIS Special Agent Basic Training and has worked as NCIS Special Agent since November 2007 and as a Department of Defense Criminal Investigator since April 2002. He has worked on a specialized unit within General Crimes and Counterintelligence investigations in Patuxent River, MD until transferred to the NCIS Middle East Field Office in 2010. Currently he is assigned to the Counterintelligence and Counterterrorism Investigation and Operations Squad – related case such as Suspicious Incidents, Compromises, Loss of Classified Matter, and Unauthorized Disclosure well as other felony level crimes. In his career, he has conducted General Crime investigations to include narcotics, sexual assault, child pornography and other crimes against persons. Based on Affiants background and training, unauthorized storage, reproduction, and dissemination of classified material and/or documents have been conducted via hard copy and through various electronic/digital sources. Additionally, short or long term possession of such classified material and/or documents is known to be stored in locations deemed private to include residences, vehicles and personal spaces. Identified residence is located in close proximity to work location and subsequent origin of classified material.

FACTS AND CIRCUMSTANCES

2. As a background, NCIS reactive investigation identified as CCN: 11APR12-MEBJ-0209-3XNA and titled S/HITSELBERGER, JAMES FRANCIS was initiated upon receipt of information via signed sworn statements from Master Sergeant Michael A. HOLDEN, Captain Brendan G. HERING, Master Sergeant Dain CRISTENSEN who observed Mr. James Francis Hitselberger, while at his place of work, physically take classified documents from a classified printer and place it into his personal backpack. Mr. Hitselberger was then observed walking out of the office carrying his backpack and the classified document that he had just placed in it. Mr. Hitselberger was followed out of the building and asked about the contents of his backpack while outside, as he was walking away from the building. Mr. Hitselberger volunteered to share the contents of his backpack which disclosed multiple documents that were classified as Secret and Secret No Foreign.

3. Based on the affiant's training and knowledge on the behavior of handling classified material and based on the totality of the circumstances surrounding the aforementioned factors and details, it is probable that the classified material and/or documents found in Mr. Hitselberger backpack was intentionally searched, printed and subsequently removed from his classified work space for unknown reasons. The backpack that was utilized by Mr. Hitselberger was also previously identified as belonging to him and seen in his passion multiple times in the past.

ITEMS TO BE SEIZED AND THEIR DEFINITION

4. Classified information to include hard copy documents, electronic/digital computer storage media, data files, to include text and graphical image files, contained on the digital storage media attached to and/ or accompanying seizure equipment (such as but not limited to computer or other devices) for investigative purposes pursuant to the investigation listed above.

5. Computer hardware described as any and all computer equipment, including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data processing hardware such as central processing units; internal and peripheral storage devices(such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage device and other memory storage devices); peripheral input/output devices; and related communication devices(such as modems, cables, and connections, recording equipment, and RAM or ROM units); as well as any devices, mechanisms or parts that can be used to restrict access to such hardware(such as physical keys and locks).

6. Computer software-described as any and all information, including any instructions, programs or program code, stored in the form of electronic, magnetic, optical, or other media that are capable of being interpreted by a computer or it's related components. Computer software may also include certain data, data fragments or controlled characters integral to the operation of the computer software. These items include but not limited to operating system software, applications software, untitled programs, compilers, interpreters, communication software, and other programming used or intended for use to communicate with computer components or in the case of peer-to-peer software always for communication and transmission of files between independent computers.

7. This data may be more fully described as any information stored in the form of electronic, magnetic, optical or other coding on computer media or on media capable of being read by a computer or computer related equipment. This media includes but is not limited to fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disk and other storage devices.

8. All electronic communications, including those previously received or transmitted, and those in transmission, or held in temporary, intermediate storage incident to transmission. The terms "records, documents, and materials, including those used to facilitate communications" as used above shall include any and all communications, previously received, transmitted, downloaded or stored. Because such communications are believed to facilitate the sharing of classified material.

9.The terms "records, documents, and materials, include those used to facilitate communications" as used above shall also be read to include any and all electronic information and/or electronic data stored in any form, which is used or has been prepared for use either for periodic or random backup or any computer or computer system. The form such information might take include but is not limited to, floppy diskettes or fixed hard drives.

10. Such electronic data in the form of electronic records, documents, and materials, including those used to facilitate communications constitutes evidence of the commission of a criminal offense. The material are therefore subject to seizure pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and the devices used to store/facilitate storage of such material may be retained as evidence in the commission of a crime for a reasonable period of time and maybe examined, analyzed, and tested for a reasonable period of time as evidence in the commission of a crime.

EXHIBIT 10

2. (U) SITREP 72 as of 082100z MAR 12, Period Covered: 072101z FEB 12 to 082100z MAR 12

3. (U) NSA, Bahrain

4. (C//REL TO USA, FVEY)

EXHIBIT 11

SECRET

SOCCENT SITREP

1. (U) JSOTF-GCC/NSWU-3

2. (U) SITREP 72 as of 082100z MAR 12, Period Covered: 072101z FEB 12 to 082100z MAR 12

3. (U) NSA, Bahrain

4. (C//REL TO USA, FVEY) [redacted]

6. (S) Commander's Comments:

[redacted]

7. (S) Operations Summary Last 24 Hours:

[redacted]

8. (S) Operations Summary Next 24 – 48 Hours:

[redacted]

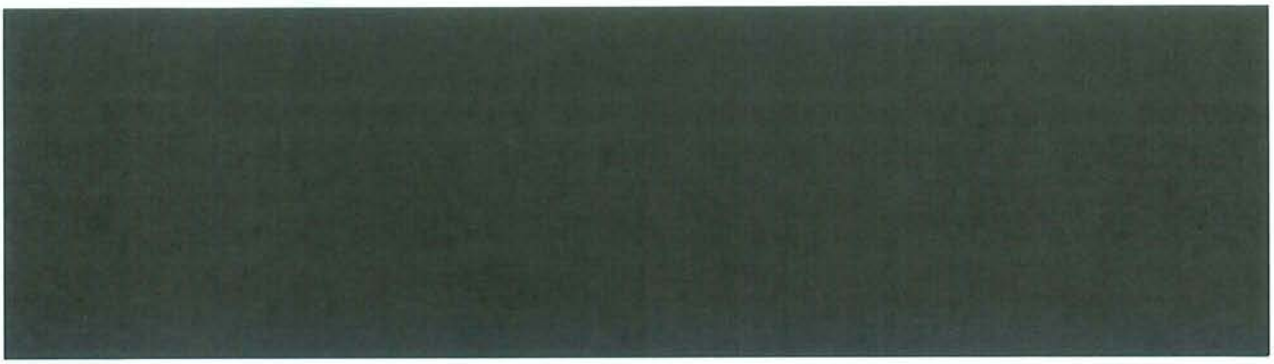
9. (U) Personnel Status, PERSTAT:

- JSOTF-GCC (NSA Bahrain):
  - 76 Assigned / 66 Present / 01 Leave / 09 TDY
- NSWU-3 (NSA Bahrain):
  - 77 Assigned / 63 Present / 04 Leave / 10 TDY
- CRE (SAN, UAE):
  - 235 Assigned / 192 Present / 0 Leave / 43 TDY

10. (S) LOGSTAT:

[redacted]

SECRET



11. (U) COMSTAT:
JSOTF-GCC/NSWU-3 JOC Chief:
P: SIPR JSOTF-GCC.JOCChief@navsoc.socom.smil.mil – GREEN
A: VOSIP 308-786-7191 – GREEN
C: DSN 318-439-3854 – GREEN
E: COMM +973 1785 3854 – GREEN
JSOTF-GCC/NSWU-3 & CRE

	STATUS		REMARKS	
CIRCUIT	JSOTF-GCC NSWU-3	CRE	JSOTF-GCC NSWU-3	CRE
NIPR			NSTR	N/A
SIPR			NSTR	N/A
CENTRIXS	N/A		NSTR	N/A
JWICS			NSTR	N/A
SATCOM/UHF/VHF			NSTR	N/A
TACSAT PRI			N/A	N/A
TACSAT SEC			N/A	N/A
TACSAT 5K			N/A	N/A
UHF LOS			N/A	N/A
VHF LOS			N/A	N/A
HF			NSTR	N/A
GBS NIPR	N/A		N/A	N/A
GBS SIPR	N/A		N/A	N/A
DVB/RCS	N/A		N/A	STANDBY
AFN			NSTR	N/A
PUBLIC INTERNET	N/A		N/A	N/A

COMMENTS:
- **CRE:** NIPRNET down due to a scheduled outage.
- **HF**: Voice: Green; Data: Yellow

12. (U) Commander's POC:

SECRET

JSOTF-GCC Operations Officer LTC David Standridge, SIPR:
standridge.david@hq.socom.smil.mil , VOSIP: 308-786-7171, DSN: 318-439-3895,
COMM: 011 (973) 1785-3123

NSWU-3 Operations Officer LCDR Rich Lozada, SIPR:
richard.lozada@navsoc.socom.smil.mil , VOSIP: 308-786-7190, DSN 318-439-8267,
COMM: 011 (973) 1785-8267

EXHIBIT 12

Email from Linda Bernard on 16May12: Subject "your collection at Hoover"

Mr. Hitselberger,

In view of the FBI investigation of your collection here at Hoover, we will no longer accept additions to the collection, as we don't want to risk receiving more classified material.
Regards,
Linda Bernard

His response on 17May12:

"My apologies. There were classified materials? I am sure that they brought unwanted excitement. Yes, there was indeed an incident in Bahrain. I was unable to locate my regular reading glasses that day over a month ago and I did not notice the 'secret' designation at the bottom. I was wearing a very narrowed rimmed pair of glasses which enabled me to read only a third of the page. The secret designation was in regular font size. I even brought the document to a sergeant's attention. He did not say anything about its classification till I was outside the building on base. He knew I had printed it out and put into my bag. When I saw NCIS, it informed me that documents of any classification were forbidden to take. Well, that is news to me. Otherwise I wouldn't have printed anything during my time there. In hindsight I think I would have simply stayed away from opening the silly classified web accounts we had, just like the other translators who really had no interest. Aside from the news summaries which we received and about which there is concern, there was nothing else that I read. Apparently these summaries were translations of Twitter feeds in Bahrain and these were done by a contract Bahraini woman. No one was really looking at the press. That is what I was doing on my own time.

My apologies indeed. It is a sad way to end.
Regards,
James Hitselberger

EXHIBIT 13

Bahrain Situation Update (13 FEB 2012)

(w/modified entries in RED bel)

COMUSNAVCENT produces the Bahrain situation update once a day at 0900Z.
SPOT Reports will be issued as conditions warrant.

(U) Executive Summary:

- (U//FOUO) Anti-g rnment protesters attempted marched towards the former Pearl Roundabout/ ouq Junction, 12 FEB 12. Mini y of the Interior (MoI) Security Forces pre ted the protesters from reach the site. An unconfirmed numb of protesters were arrested. njuries were reported.
- (U//FOUO) Shi'a y h reportedly engaged in isolate low-level, unlawful behavior in 28 dist s throughout Bahrain, 12 FEB Bahraini Press reported an unconfirmed nu er of arrests. No injuries were ported.
- (U//FOUO) Bahrai leading Shi'a newspaper claim the MoI Director intends to increase the nur er of MoI checkpoints through the island as of 13 FEB 12. The MoI media site as not corroborated this report
- (C//REL TO USA, A J) [redacted]
- (U//FOUO) There continues to be no known specific or credible threats to U.S./Coalition forces or bases.

(U) Current Developments:

- (U//FOUO) A large ntingent of protesters attemp to march towards the former Pearl Roun bout/Farouq Junction from div ent routes at 1630C, 12 FEB 12. MoI Secur Forces prevented the proteste rom reaching the site by repelling the prote rs with teargas. All protesters re effectively disbursed by 1830C. Bahrain ess reported no injuries, but c irmed the MoI conducted an unknown numb of arrests.
- (U//FOUO) Pro-go nment press reported the pro ent Shi'a blogger, Zainab Al Khawajah was a sted for disturbing public secu while attempting to march towards the rmer Pearl Roundabout/Farou nction, 12 FEB 12. Ms. Al Khawajah, a well-k wn blogger, was reported to b the custody of the Capital Governora olice while awaiting referral t e Public Prosecutor.
- (U//FOUO) Shi'a y h continue to engage in low-le , unlawful behavior. Activity was obser in the following areas, 12 FEB
  - A'Ali, Abu S a, Adhari, Al Daih, Al Duraz, Al likiyah, Bilad Al Qadeem, Bani Jamra oori, Dar Kulaib, Demistan, Di Eker, Hamala, Jeblat Hebshi, Jid fs, Karbabad, Karranah, Khami Ma'ameer, Naim, Saar, Salihiya, Sa ois, Sehla, Shahrakkan, Sitra, Q yyah,

- Activity con ed of youth blocking roads lea g into Shi'a villages with makeshift b iers. Youth reportedly engage lol Security Forces with Molotov co ails, rebar, and stones. Mol re nded in kind with tear-gas to disbu protesters. Press reported th lol conducted a number of arrests, b no amplifying data was provid No injuries were reported.

- (C//REL TO USA, ACGU) [redacted]

(U) Assessments:

- (U) There continues to be no direct threat noted to US or Western interests in Bahrain. The greatest threat to US or Western personnel is collateral damage or unintended consequences from protestor or security forces activity.
- (U) Estimate an increase in both Sunni and Shi'a protest activity to occur over the next 48 hours. Shi'a protesters will likely attempt to march on and reoccupy the former Pearl Roundabout/Farouq Junction on 14-15 FEB 2012. Ministry of the Interior (MoI) Security Forces are well positioned to prevent protesters from reaching this symbolic site. Potential Sunni demonstrations could mirror Shi'a activity in size, scope and intensity. There exists the possibility for an increase in sectarian violence in the near-term. The MoI maintains the capability and will to prevent violent demonstrations from spilling out of the traditional protest areas.

(U) Unknowns:

- (S//REL TO USA, FVEY) [redacted]
- (S//REL TO USA, FVEY) [redacted]
- (S//REL TO USA, FVEY) [redacted]

- (S//REL TO USA, FVEY) [redacted]
- (S//REL to USA, FVEY) [redacted]

(U) **Current Measures**:

- (U//FOUO) FPCON BRAVO plus additional measures.
- (U) The Ghuraifa area of Juffair, to the north of the Department of Defense Dependents' School and to the west of the area known as "American Alley" has been placed off-limits from 2000C – 0400C until further notice. Essential travel along Juffair Avenue, the southern boundary of this area, is authorized during those hours.
- (U) No foot or bicycle traffic is permitted between Mina Salman pier and Naval Support Activity Bahrain; only liberty busses will be used by Sailors from visiting ships.
- (U//FOUO) AMEMBASSY Manama Warden Message advises all Americans to avoid demonstrations and certain geographic areas identified on the AMEMBASSY Manama website until further notice.
    - (U) On 23 JAN 2012 the Department of State updated its Travel Alert for Bahrain to inform U.S. travelers of current conditions; the advisory will expire 19 APR 2012. The Alert notes that spontaneous demonstrations could turn violent with little to no notice. The alert adds that unrest is commonplace in certain neighborhoods, especially during weekends and after dark.

(U//FOUO) Demonstration notices may be found on the AMEMBASSY Manama website at http://bahrain.usembassy.gov/demonstration.html

EXHIBIT 14

AS OF 141825DAPR05

SUMMARY: FIVE VEHICLES ARE GATHERING FOR AN ATTACK NEAR QAQA ROAD SOUTH OF FOB LUTAFIYAH

DETAILS: FIVE VEHICLES ARE GATHERING FOR AN ATTACK NEAR QAQA ROAD SOUTH OF FOB LUTAFIYAH

THE VEHICLE ARE IDENTIFIED AS FOLLOWS:

- **A. (S/REL TO USA AND MCFI)** [redacted]
- **B. (S/REL TO USA AND MCFI)**
- **C. (S/REL TO USA AND MCFI)**
- **D. (S/REL TO USA AND MCFI)**
- **E. (S/REL TO USA AND MCFI)**

ALL THE VEHICLES ARE GATHERING ON A DIRT ROAD NEAR QAQA ROAD VICINITY //MGRS COORD: 396/468//. THERE ARE THREE TO FOUR PERSONNEL PER VEHICLE AND THEY ARE PREPARING FOR AN ATTACK ON AN UNKNOWN TARGET ON OR NEAR FOB LUTAFIYAH //MGRS COORD: 38S MB 399 480//.

EXHIBIT 15

James Hitselberger
5272 Boaz Road
Covesville, VA 22931

July 8, 2005

Dear Mr. Bauer,

I am on temporary leave from Iraq and I just received your letter, dated March 28, 2005. It had been forwarded from Karbala, Iraq, where you sent it. I have since been posted in Babylon Province, just south of Baghdad, and, most recently, in Fallujah. I will return to Iraq at the end of this month and receive yet another assignment.

I am enclosing three intelligence reports for your archives. These are all from Fallujah. I was at the main check point for entering Fallujah and in the compound there is a box containing reprints of AMerican news reports about Iraq. For some reason or other, someone put these intelligence reports inside along with the newspaper articles. Two of the reports have no classification and the third is classified as "secret." It states that it will be declassified on 20150323. Could that mean ten years from the date it might be issued? That is, March 23, 2015?

Regardless of the case, this material seems to warrant archival preservation. I will leave the matter up to you to determine when researchers can have access to these items, as I am fully confident that your institution balances national security concerns with the need of researchers for original source material.

sincerely,

James Hitselberger

EXHIBIT 16

CA - HITSELBERGER

HOOVER INSTITUTION
ON WAR, REVOLUTION AND PEACE
Stanford, California 94305-6010

HOOVER INSTITUTION
STANFORD UNIVERSITY

...ideas defining a free society

September 13, 2005

James Hitselberger
5272 Boaz Road
Covesville, VA 22931

Dear Mr. Hitselberger,

Thank you very much for the additional material from Iraq that you sent to us in early July. I'm sorry that I wasn't able to respond to you sooner, and hope that this letter reaches you, since you mentioned that you were heading back to Iraq at the end of July.

Since the items that you sent are classified, they will be treated as such, and segregated from the rest of your collection and stored in our vault until the time when they are able to be declassified. However, I do agree that they warrant preservation and I am glad that you sent them to us. Once these documents have been declassified, they will be returned to your collection, and be made available for research use.

In the meantime, as ever, please feel free to send us other items that you think might be of interest to us. I realize that with the changes in your assignments, it might be hard to reach you, but nevertheless please know that we appreciate the items that you send to the archives. Thank you are taking the time to do this, especially in light of the how busy you must be and how many other pressing matters must occupy your attention these days.

With best wishes,

Sincerely,

Brad Bauer

Brad Bauer
Associate Archivist for Collection Development