Axiologic Solutions, LLC
Annual Security Training

Axiologic Solutions, LLC
Security Team

* Facility Security Officer – Roselita Berta

  (703) 922-5500 ext. 708 (o)

  (804) 742-2567 (c)

  Roselita.Berta@axiologicsolutions.com

* AFSO – Thomas Stauber

  Thomas.Stauber@axiologicsolutions.com

* AFSO – Rob Wittmaack

  Robert.Wittmaack@axiologicsolutions.com

Topics

* Counterintelligence and Threat Awareness
* Insider Threat
* Operational Security
* Accessing Classified Information
* Need-to-Know
* Document Control and Couriering Responsibilities
* Personnel Security
* Reportable Information
* Information Systems Security
* Visitor Control and Facility Information

Counterintelligence & Threat Awareness

Counterintelligence: Activities designed to prevent spying, intelligence gathering and sabotage by an enemy or other foreign entity.
As cleared defense contractors, we work in highly sensitive arenas that are constantly targeted for intelligence collection by our adversaries. We must be aware that threats to national security information, both foreign and domestic threats, do exist.

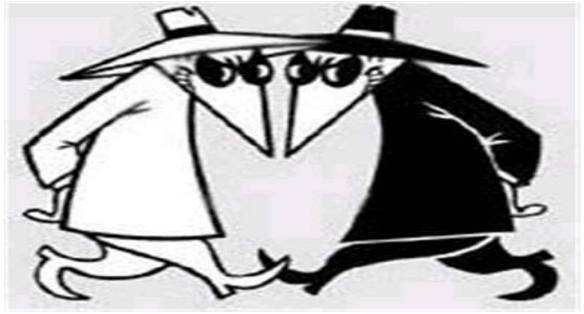
One of the best ways to counter threats is to *know our adversaries* and their *targets*, and know how to protect ourselves and the information we have access to both here in the U.S. and while on travel.

Through proper counterintelligence practices, we can counter adversarial intelligence and espionage efforts.

The Adversaries

Who are the spies?
Some Examples:

* Potential Employees
* Potential Clients
* Students/interns doing research in the U.S.
* Media Personnel
* The Neighbor
* Members of professional organizations
* Foreign Entities/corporations/visitors
* Competitors
* Trusted insiders
* Disgruntled or greed motivated U.S. citizens



Adversaries could be posing as anyone

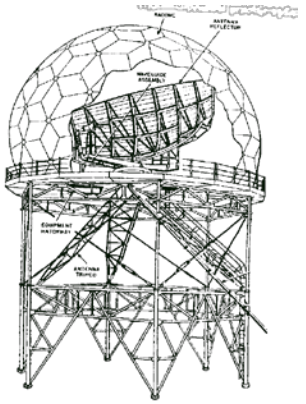
Motives

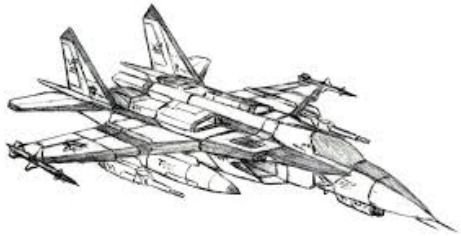
* Greed or Financial Need
* Anger or Revenge
* Problems at work
* Ideology/Identification
* Alliance to another country
* Adventure/Thrill
* Vulnerability to blackmail
* Divided Loyalty
* Ego/Self Image
* Family problems.

Top 10 Targeted Technologies in FY18

Classified & Unclassified

* **Aeronautics** Design & Manufacturing of air flight machines, and the techniques of operating aircraft & rockets
* **Command, Control, Communications, & Computer (C4)**
* **Electronics** Hardware
* **RADAR Systems**
* **Armaments & Survivability** Weapons & Material Research/ Development
* **Lasers & Optics** Behavior and properties of light
* **Sensors** Detect events or changes in its environment, and then provide a corresponding output
* **Marine Systems** Submarine communications
* **Positioning, Navigation, & Time** GPS Technology
* **Materials & Processing** Techniques used in manufacturing /transforming componer





Foreign Intelligence Service

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS

San Francisco Division

Home • San Francisco • Press Releases • 2015 • Chinese Professors Among Six Defendants Charged with Economic Espic

Twitter (38) Facebook (1) Share

Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China

Chinese Professors Alleged to Have Stolen Valuable Technology from Avago Technologies and Skyworks Solutions to Benefit a PRC University

U.S. Department of Justice
May 19, 2015

Office of Public Affairs
(202) 514-2007/TDD (202) 514-1888

On May 16, 2015, Tianjin University Professor Hao Zhang was arrested upon entry into the United States from the People's Republic of China (PRC) in connection with a recent superseding indictment in the Northern District of California, announced Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Melinda Haag of the Northern District of California and Special Agent in Charge David J. Johnson of the FBI's San Francisco Division.

The 32-count indictment, which had previously been sealed, charges a total of six individuals with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain U.S. trade secrets for the benefit of universities and companies controlled by the PRC government.

"According to the charges in the indictment, the defendants leveraged their access to and knowledge of sensitive U.S. technologies to illegally obtain and share U.S. trade secrets with the PRC for economic advantage," said Assistant Attorney General Carlin. "Economic espionage imposes great costs on American businesses, weakens the global marketplace and ultimately harms U.S. interests worldwide. The National Security Division will continue to relentlessly identify, pursue and prosecute offenders wherever the evidence leads. I would like to thank all the agents, analysts and prosecutors who are responsible for this indictment."

"As today's case demonstrates, sensitive technology developed by U.S. companies in Silicon Valley and throughout California continues to be vulnerable to coordinated and complex efforts sponsored by foreign governments to steal that technology," said U.S. Attorney Haag. "Combating economic espionage and trade secret theft remains one of the top priorities of this Office."

On the one year Anniversary of the U.S. indictment of five Chinese officials the DOJ charged another six Chinese citizens with espionage. This time they are under arrest and in U.S. custody

U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage

First Time Criminal Charges are Filed Against Known State Actors for Hacking

U.S. Department of Justice
May 19, 2014

Collection Methods

How are you targeted?

* Cyber Attacks:
* Seeking Employment:
* Solicitation/Marketing of Services: Foreign-owned companies seek business relationships with U.S. firms that enable them to gain access to sensitive, or classified information, technologies or projects.
* Request for Information: The most frequently reported method, provides the greatest return for minimal investment & risk. Direct & indirect requests (emails, phone calls, conversation) in attempts to obtain valuable data. A simple request can get a piece of information helpful in uncovering a larger set of facts.
* Acquisition of Technology: collectors exploit direct & indirect acquisition of technology and information via Third Parties, front companies, direct purchase of U.S Firms or Technology
* Public Venues: Conferences, conventions, symposiums, trade shows offer opportunities for foreign adversaries to gain access to U.S. information & experts in dual-use & sensitive technologies.
* Foreign Visitors: Opportunity to collect inside information during visit
* Social Media : Catfish - someone who pretends to be someone they are not
* Foreign Targeting of U.S. Travelers: Elicitation information during innocuous conversations, eavesdropping on private telephone conversations, downloading information from laptops/digital storage devices.

The six regions most frequently affiliated with validated Suspicious Contact Reports are:

East Asia, Near East, Europe/Eurasia, South & Central Asia, Africa, Western Hemisphere

Stolen Technology

B1 Bomber

F-15 Fighter

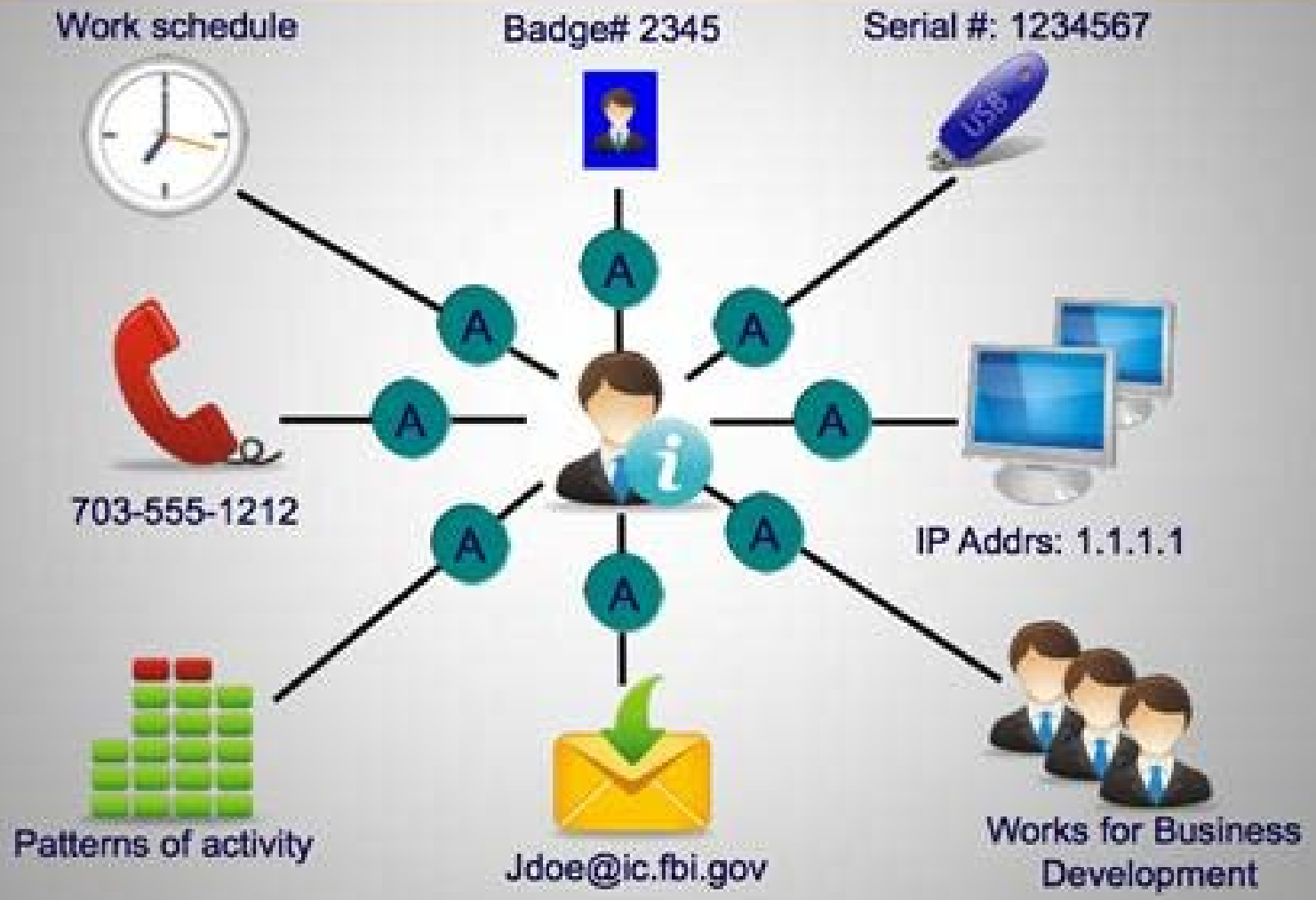
AWACS

20 + years of R&D = Millions $
Locates and destroys incoming missiles

AEGIS Radar System

50+ years of R&D = Trillions $
Used for Surveillance, Reconnaissance & Defense

Do You Know Your People?



Insider Threat

12 Key Behavioral Indicators to look out for:

* Takes proprietary or other material home - via documents, thumb drives, computer disks, or e-mail.
* Seeks or obtains proprietary or classified information on subjects not related to their work duties.
* Interest in matters outside the scope of their duties related to foreign entities
* Unnecessarily copies material, especially if it is proprietary or classified.
* Remotely accesses the computer network while on vacation, sick leave, or at other odd times.
* Disregards company computer policies
* Works odd hours without authorization; notable enthusiasm for overtime work and weekend work
* Unreported foreign contacts or travel
* Short trips to foreign countries for unexplained or strange reasons.
* Unexplained financial affluence
* Engages in suspicious personal contacts, such as with competitors or other unauthorized individuals.
* Overwhelmed by life crises or career disappointments.
* Concern that they are being investigated; leave straps to detect searches of their work area or home; searches for listening devices or cameras. (PARANOIA)

Threat

2015 Navy Engineer Sentenced for Attempted Espionage

Mostafa Ahmed Awwad passed Information on Latest Aircraft Carrier to Undercover Agent in regards to the USS Gerald R. Ford—to an individual he thought was an Egyptian intelligence officer. His actions could have potentially compromised the safety of some 4,000 American sailors. Awwad was sentenced to 11 years in prison after pleading guilty in 2015 to attempted espionage.

2010 Disgruntled Employee Michael Mitchell

Michael Mitchell became disgruntled and was fired from his job due to poor performance. He kept numerous computer files with his employer's trade secrets, then entered into a consulting agreement with a rival Korean company and gave them the stolen trade secrets. In March 2010, he was sentenced to 18 months in prison and was ordered to pay his former employer over $187,000

Edward Snowden
NSA

Robert Hanssen
FBI

PFC. Manning
Army

Protecting Information

Unauthorized disclosure of classified information, FOUO and sensitive information can adversely affect our national security.

What are we protecting?

Classified Information

* US Government Classified material (Top Secret, Secret, Confidential and unclassified but sensitive information).

Company Proprietary Information

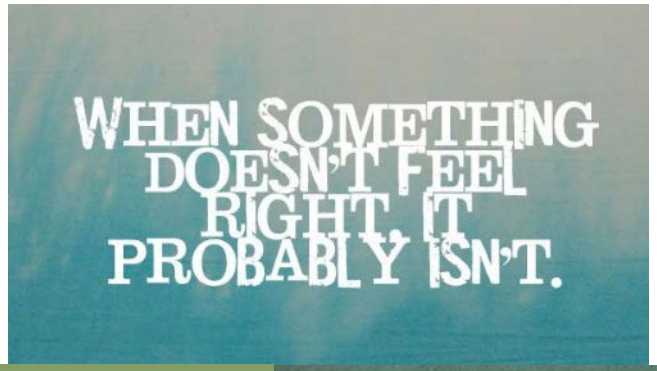
* financial compensation of employees, corporate financial investments and resources, personnel ratings, corporate budget information.
* trade secret information, competitive relationships, corporate security vulnerabilities.

Personally Identifiable Information (PII)

* name, Personal Identification Number, SSN, Drivers License, Passport #,

biometric identifiers (x-ray, retinal scans, fingerprints), financial Information (bank account, credit/debit card), medical records, education records, employment records, authentication information (passwords, information to re-enable passwords).

What to do???



* Report it to your FSO

No amount of information is insufficient

Operational Security (OPSEC)

* What is OPSEC?

* - Identify the Critical Information
* - Analyze Threats
* - Discover Vulnerabilities
* - Assess Risks
* - Develop Countermeasures

* What Information should I protect? Information that the adversary needs to accomplish their mission (to include Intelligence information on programs associations and technical information on communications.

* - Military weapons information (capabilities, manufactures, purpose, vulnerabilities, effectiveness, type, testing details)
* - Scientific Industrial Information (technology & research, technical specs, marketing plans, key personnel, breakthroughs)

OPSEC & Defensive Security Measures

Operations Security (OPSEC)

The practice of keeping potential adversaries from discovering sensitive unclassified information. It protects operations planned, in progress, and those completed.

- Putting unclassified pieces together *can* reveal critical or sensitive classified information which can be used to cause harm to the United States and its allies
- Trained Foreign intelligence collection officers are looking for the "pieces of the puzzle" to add to the big picture

Defensive Security Measures

Be vigilant to both internal (*the insider threat*) and external threats

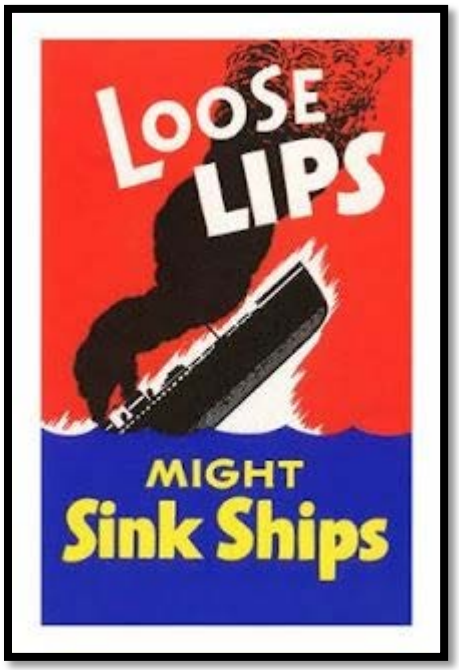
Using caution when in contact with foreign nationals, whether domestically or when on foreign travel

- The insider threat is one of the most dangerous that we face.
- Most common flags of insider threat are unexplained wealth, unexplained /un reported foreign travel, attempts at accesses classified information of which someone does not have a need to know.
- Identify suspicious activities or collection attempts and report them immediately to security

Be Vigilant & Be Cautious!

Trained Foreign Intelligence collection officers are looking for the "pieces of the puzzle" to add to the big picture.

* Talking around classified
* Social Media
* Visual Indicators
* Foreign Travel
* Sharing information with personnel that don't have a "Need to Know"
* Non Discussion areas (i.e. breakroom)



Good OPSEC? NO

OPSEC: Foreign Travel

Don’t make you or your family a target…

* Do not draw unnecessary attention to yourself. For example, avoid wearing USA, military, company or customer apparel
* Do not discuss specifics about your job to people you meet
* Know the location of and how to contact the nearest U.S. Embassy
* Company and government customer laptops and cell phones should not be taken outside of the country. Your company may be able to provide a sanitized laptop and/or cell phone for you before you travel.

Foreign Travel Reminders

* Be aware of your environment and the possible situations that could arise. It's important to never forget that you're in a foreign country. The laws that protect you in the United States may not travel with you.
* Limit sensitive discussions – hotel rooms or other public places are not suitable to discuss sensitive information.
* Ignore or deflect intrusive inquiries or conversation about business or personal matters
* Do not divulge information to anyone not authorized to hear it
* Do not publicize travel plans & limit sharing of this information only to people who have a need-to-know
* Keep hotel room doors locked. Note how the room looks when you leave.
* Remember that you may be on the Government Cellular Network of the country you're visiting. Be aware of the information you're discussing (and typing).
* Report any suspicious activities, incident or contacts to your FSO when you return.
* Do not use computers or faxes at foreign hotels/business centers for sensitive matters
* If you're taking a company provided mobile device with you, you must coordinate with your security officer to ensure the device is properly protected

Foreign Travel

Foreign Travel Steps

1) Notify your FSO at least 30 days in advance. Fill out pre-travel and post travel paperwork. (*personal and business trips*)

2.) Visiting a Foreign Embassy is considered Foreign Travel

- You are on sovereign foreign ground of the host country.

3.) Foreign Cruise ports are reportable

- report stops if the cruise originated from a U.S. Port

****Contact your Facility Security Officer upon your return to conduct a debriefing from your trip.

Smart Traveler Enrollment Program

Benefits of Enrolling in STEP:

- Review the Preparing for a Trip Abroad at the **http://www.state.gov/travel/**
- Sign up for the *Smart Traveler Enrollment Program - STEP* (located under the Resources Heading)
- The Smart Traveler Enrollment Program (STEP) is a free service to allow U.S. citizens and nationals traveling abroad to enroll their trip with the nearest U.S. Embassy or Consulate.
- Receive important information from the Embassy about safety conditions in your destination country,
- Help the U.S. Embassy contact you in an emergency, natural disaster, civil unrest, or family emergency.
- Help family and friends get in touch with you in an emergency

Anyone can join when traveling abroad

Accessing Classified Information

Non-Disclosure Agreements

Required to sign a Non-Disclosure Agreement (NdA) before receiving classified access . It is an agreement between you and the United States Government that states you will not disclose classified information to individuals without both the required clearance level and a Need to Know.

<u>Types of NdA's:</u>

- SF312 for DoD/Collateral
- Form 4414 for SCI

Violation of the Agreement:

- Loss of your clearance/access
- Loss of employment
- Criminal Charges

NDA's are binding for life

Need - to – Know (NTK)

1) Need-to-Know (NTK) is the most important concept one needs to practice when working with classified material. The NTK requires you, the custodian of classified and/or proprietary information to establish (prior to disclosure) that the intended recipient must have access to the information to perform his or her official duties
2) As a cleared employee, you have the responsibility to confirm a recipient's NTK, and the authority to grant or deny access to classified information for the program which he/she is performing official duties.
3) As a cleared employee, you have the responsibility to verify a recipient's NTK, and the authority to grant or deny access to classified information for the program which he/she is performing official duties.
4) Each individual – regardless of rank/position or amount or clearances/accesses only has a NTK for information pertinent to the performance of their specific task/project.
5) Data Owners (Government) determine the NTK

NEED-TO-KNOW IS NOT THE SAME AS WANT-TO-KNOW

Confirming or Denying

- Confirming or denying something you see on TV, read on the internet or heard in conversation that may have similarities to classified information or projects is an unauthorized disclosure of classified information.
- Do not confirm, deny, or comment
- Do not access websites that claim to host classified information

> Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information."
> - E.O. 13526, Section 1.1(4)(c)

Document Control

3 Levels of Classification for National Security Information and the levels of damage to National Security associated with each if there is unauthorized disclosure:

TOP SECRET **GRAVE DAMAGE** to national security

SECRET **SERIOUS DAMAGE** to national security

CONFIDENTIAL **DAMAGE** to national security

- Contact your SSO or PSO and consult classification guides for specific use of these classifications

- Controlled Unclassified Information[1] : For Official Use Only (FOUO) or Sensitive But Unclassified (SBU) materials are not classified, but dissemination is still restricted. Documents must be portion marked.

- What is important to remember is that *all* classified and sensitive information requires protection from unauthorized disclosure

Controlling & Storing Classified Information

* Use the appropriate coversheets at all times
* Always ensure it is under the control of or guarded by an authorized person or stored in the appropriate GSA approved containers when not in use
  - Security must provide safe and combination access
  - Safe combinations are classified at the same level of the information. (Do not write combinations down)
  - Do not co-mingle or store DoD, SAP, SCI or Foreign information without proper coutilization agreements.
* Never view classified documents in public places, only at government organizations or approved areas of contractor facilities.
* Only process and destroy on approved and appropriately marked equipment.
* Inventoried items can only be destroyed by Security

Couriering

Pre-coordinate with Security:
(the contract may not allow contractors to courier)

Purpose:

- Security will ensure the facility is cleared to accept the package
- Ensure you carry your courier letter or card at all times when hand carrying classified material.

Responsibility:

- Use extraordinary care and judgement while in transit
- Travel Direct (NO stops!)
- Ensure the package stays in your possession at all times
- Confirm the cleared individual is at the facility to receive the package immediately upon arrival
- Report any trouble during transit

Classifying Material

2 Ways material is classified

1) ORIGINAL CLASSIFICATION

As defined in Executive order 13526, only certain U.S.

Government agencies can originally classify information.

2) DERIVATIVE CLASSIFICATION

The act of incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the developed material consistent with the markings of the source information.

Cleared employees can only derivatively classify information

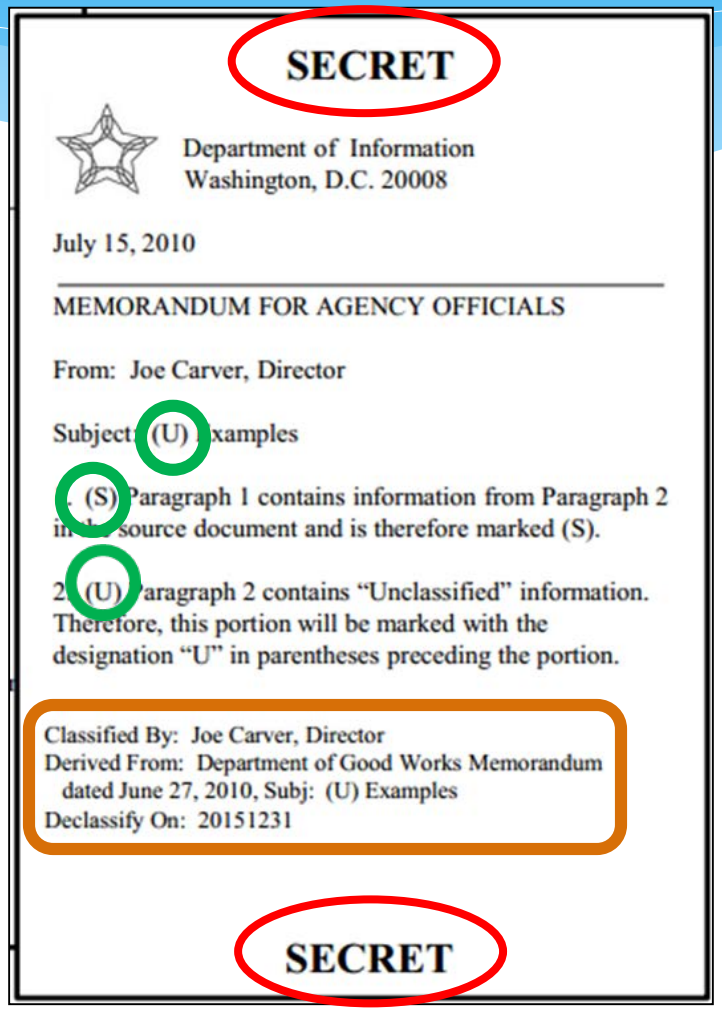
Marking Derivatively Classified Documents

Why do we mark:

- To identify & protect classified information
- Alert the reader (overall classification)
- To facilitate the sharing of information among agencies
- To aid in future review & release of documents
- Identify which portions contain classified info (portion marking)
- Specify the source using the appropriate Security Classification Guide (classification authority)
- E.O 13526 & ODNI CAPCO document mandates that all classified material be portion marked

How Do We Mark?

- • Portion marking (paragraphs, charts, tables, pictures, titles, etc.)
- • Overall classification of document
- • Identification of classification authority
- • Reason for classification (cited from Sec 1.4 of E.O. 13526, as amended)



SECRET

Department of Information
Washington, D.C. 20008

July 15, 2010

MEMORANDUM FOR AGENCY OFFICIALS

From: Joe Carver, Director

Subject: (U) Examples

(S) Paragraph 1 contains information from Paragraph 2 in the source document and is therefore marked (S).

2. (U) Paragraph 2 contains "Unclassified" information. Therefore, this portion will be marked with the designation "U" in parentheses preceding the portion.

Classified By: Joe Carver, Director
Derived From: Department of Good Works Memorandum dated June 27, 2010, Subj: (U) Examples
Declassify On: 20151231

SECRET

Personnel Security

* There are three levels of security clearance and access:
    - Top Secret – Reinvestigation occurs every 5-6 years
    - Secret – Reinvestigation occurs every 10 years
    - Confidential – Reinvestigation occurs every 15 years
* Security tracks all investigation timelines and will notify you when you are due for your periodic reinvestigation (PR)
* Electronic Fingerprints are due for Initial (and some Periodic Reinvestigations)
* OPM – PR can be submitted 90 days prior to 5-6 year
* Agencies may request a new SF-86 at any time due to security concerns

Polygraph Information

* Individuals with SCI access may be subject to a polygraph examination
* Polygraphs do not coincide with PR's
* Contact Security if you are requested to take a polygraph
* If you decline to take a polygraph, you will be removed from access

3 Types:

Counter-Intelligence (CI)

Lifestyle (LS)

Full Scope = CI + LS

Reportable Information

Information is Confidential…

* **SIGNIFICANT LIFE CHANGES:**
* - Change in name, change in marital status (including legal separation)
* - Adoption, cohabitation, Intent to marry a foreign national
* - Change in citizenship status, desire to no longer hold access to classified information
* - unwillingness to submit to a background investigation or polygraph examination.
* **FOREIGN TRAVEL (Pre/Post)**
* **COMPUTER MISUSE:**
* - sharing passwords
* - modifying/destruction/manipulation of hardware or software on government or contractor equipment.
* - Obtaining or sharing someone's password/account
* Security violations (loss of classified information, unreported violations.

If it's on your SF86, you must report it. When in doubt; ask Security!

1 The Office of Personnel Management has not updated the SF-86 to reflect the change in question #21 to include sexual assault but has published Notice No 13-02

Adverse Information Reporting

Adverse information (AI) is anything that reflects unfavorably on the trustworthiness or reliability of the employee and suggests that their ability to safeguard classified information may be impaired.

WHAT TO REPORT

* **EXCESSIVE FINANCIAL CHANGE**
* - Unexplained affluence: Inheritance, large gifts, lottery winnings
  - Liens, wage garnishments, judgments, bankruptcy, late payments (90+ days overdue)
  - Short sales, foreclosures
* **VIOLATIONS OF LAW/ARREST**:
* - civil court actions (ANY involvement with police, regardless of whether there's a conviction.
* - traffic citations of $300 or more
* - Any attempts of blackmail or coercion

ALCOHOLISM and/or ALCOHOLISM TREATMENT:

- Arrests, treatment and/or counseling

* **EMOTIONAL/MENTAL HEALTH CONSULTATIONS:**
* - psychological counseling (*not* to include marital, family, grief, SA[1] or related to adjustment from service in a military combat environment)
* **ILLEGAL DRUG USE**:
* - Illegal/improper use of narcotics, non-medicinal drugs, non-prescription drugs, or controlled substances.
* - Federal Law supersedes states law. States that have enacted laws authorizing the use, possession, production, procession & distribution of marijuana is not condoned when holding a clearance and will be reported as adverse information.

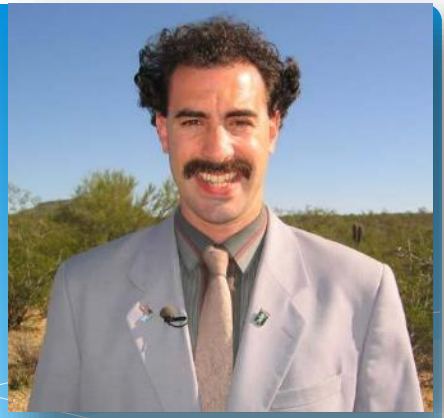
Security Violations & Incident Reporting

Report security violations immediately to both Security and the on-site customer security representative (if applicable). Quick reporting can help protect further loss. For example, if there is a classified data spill on a network, the quicker it is reported, the better chance there is to limit contamination.

Examples of Violations:

* Personal Electronic Devices (PEDs) in unauthorized areas
* Improperly storing classified information in a desk or unauthorized cabinet
* Discussing classified information in a public area, (lobbies, cafeterias, airports)
* Leaving classified information unattended in an unsecure area
* Failure to follow appropriate procedures for destruction of classified material
* Unauthorized access or inadvertent disclosure
* Removing classified from SCIF (taking it home on accident)
* Data spill (originated from non-employee)
* iPad, FitBit, cell phones brought into SCIFs
* Sharing unattended account
* Special Access Program (SAP) information transmitted on a lower classified level system
* Classified information spilled onto an unclassified network
* Inadvertent removal of classified material
* Shared computer accounts
* Loss, compromise, (or suspected loss or compromise) of classified information
* Evidence of tampering with a security container used for storage of classified information

Foreign Contacts



REPORT close and continuing foreign contacts to Security

Roommates
Family Members
Previous Co-Workers
Social Networking Sites

* Foreign Contact Forms are available form Security and your Government SSO
* Only have to report Foreign Contacts 1x and/or as required by the Government Customer
* Contacts are not only face-to-face (U.S. mail, email, chat rooms, social media sites, telephone, webcam are considered methods of contact).
* Reminder: as a cleared individual with access to sensitive and classified information, it is your responsibility to ensure that any attempts by Foreign Nationals to elicit information regarding your work are reported to Security

Suspicious Contacts

"Suspicious contacts include, but are not limited to, any individual making an effort to gain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared contractor employees with known or suspected intelligence officers from any country, or any contact which suggests that an employee may be the target of an attempted exploitation by the intelligence services of another country shall be reported to your Facility Security Officer (who will report to DSS) and to the FBI if actual, probable or possible espionage, sabotage, terrorism or subversive activities at any locations."

WHERE?

Encountered at seminars, conferences, trainings, public places

HOW?

Be alert, stay vigilant! Report suspicious contacts to Security!

Report Suspicious Contacts……..

Information Systems Security

Data Spill: If you believe you have classified data on your unclassified network:

1. **STOP**
2. **DISCONNECT**
3. **DO NOT DELETE**
4. **DO NOT FORWARD**
5. **CONTACT SECURITY**

SpearPhishing

Norton: *"Spear phishing is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC."*

* Email appears legitimate, sent from the right person, grammar, punctuation
  Roselita.Berta@axiologicsolutions.com
* Do not click on links or attachments
* Call the FSO
* After all else, SHIFT+DELETE the email

Information Systems Security

What to do?

* Do not connect classified systems to an unclassified system or network
* Use strong passwords
* Classified Information Systems (IS) passwords are *classified!*
* Do not write down passwords
* Do not share passwords
* Use a unique password on each IS.

  For example, your GWAN password cannot be the same as your CWAN password.
* Lock your screen when not in use to prevent unauthorized access
* Audit trails show events on your computer. Do not let someone else access information on your account – you are responsible for actions taken on your account!
* Sharing accounts for any reason is prohibited
* Under no circumstance are users allowed to introduce software to an Information System without prior approval
  - Users must provide a written request to the ISSO
  - Complete a Media Installation Request Form

Visitor Control & Facility Information

Incoming Visitors

* All visitors must sign in while visiting a facility
* If issued a Visitor Badge, it must be displayed at all times during the visit

Sending a Visit Request

Required Information includes:

* Full Name
* Dates of Visit
* Clearance Level required
* Technical POC Name/Number
* Security POC Name/Number
* Location of Visit
* SMO Code (if applicable)
* Justification of Visit

"You should've called first – given me a chance to not be home."

Preparing for Foreign Visitors

* Ensure your staff know what can/cannot be discussed
* - - There are general restrictions on technical discussions & access to technical materials (even at the unclassified level). Keep the discussions to an agrees-upon topics and information.
* - - Escorts should conduct a walkthrough of the facility prior to the visitor arriving to ensure they will not have audible or visible unauthorized access. Escorts need to maintain visual contact with all visitors at all times.
* Foreign Visitors should not use company IT systems or faxes.
* Report any suspicious incidents to the FSO.
* Foreign National Visitors need to be coordinated 30 days in advance of their visit with the Facility Security Officer.
* - - The FSO must contact the DSS Representative to pass along the visitor information.
* Foreign nationals showing up unannounced is an intelligence collection method and must be reported to DSS.

Preparing for Foreign Visitors

Techniques

* Peppering: Visitors asking the same question in different styles or one visitor asking the same questions to multiple U.S. contractor employees
* Wandering Visitor: The visitor uses the distraction provided by a large delegation to slip away, out of the control of the escort.
* Divide & Conquer: Visitors take a U.S. person into different areas to discuss issues in order to derive the U.S. Person of their safety net of assistance in answering questions.
* Switch Visitors: A collector added to the group without leaving enough time for a background check on the new visitor.
* Bait & Switch: The visitors say they are coming to discuss business that is acceptable for discussion, but after they arrive their agenda switches to different questions & discussion topics.
* Distraught Visitor: When the visitor's questions are not answered, he/she acts insulted or creates an uncomfortable scene in the attempt to psychologically coerce information from the target

SCIF Security

* Remember to check your pockets, briefcases, purses, backpacks, etc. for any prohibited items before entering a SCIF

* If you plan to work before or after normal business hours please coordinate with your local security officer (if allowable)

* Individuals are subject to search at any time. Please cooperate with Security if you are asked to have your belongings checked for prohibited items. This is a government requirement that must be fulfilled

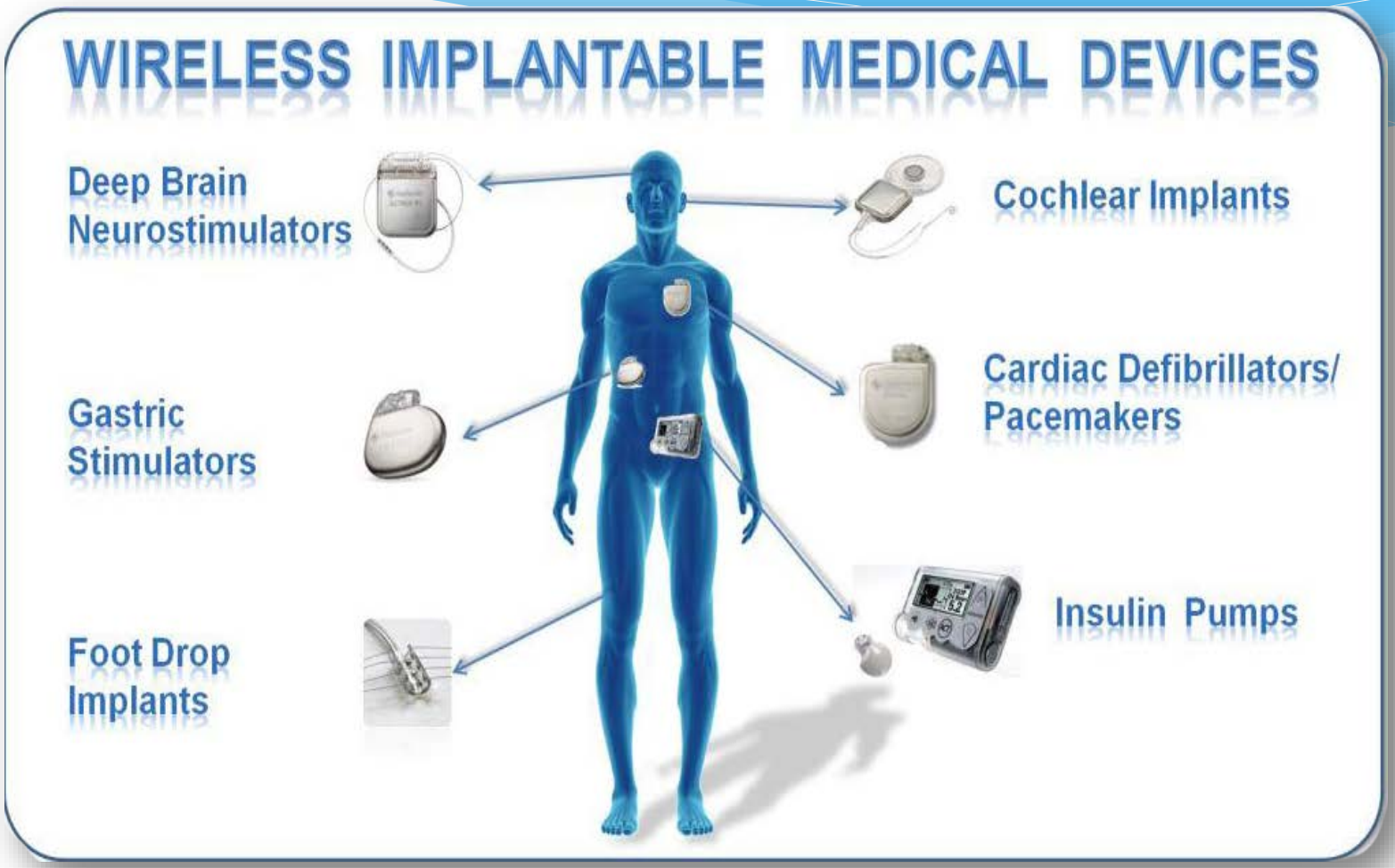
Prohibited in a SCIF

Sometimes Prohibited

**** You must get approval from the SCIF Owner prior to bringing in any device ****

Sometimes Prohibited

** You must get approval from the SCIF Owner prior to bringing in any device **



Emergency Response Plan

Your life safety is the _____ priority in the event of an emergency.

If possible:

* Secure all classified materials
* If the step above cannot be completed while maintaining your personal safety, exit the building immediately and notify security.

Fraud, Waste & Abuse Reporting

Summary

- **When in doubt ask Security** - If you are unsure of a specific procedure or unsure of a requirement please contact security
- If your on site Security Officer is unavailable contact any member of Security for assistance.
- Report any foreign or suspicious contacts regardless of their citizenship
- All foreign travel must be reported. If you are briefed through the and of the 3 Letter Agencies, they also require notice. Please see security for assistance
- Make sure all visitors sign in at the front desk. All visitor's clearance and access levels must be verified by Security before granting them access to secure spaces at any facility.
- Alert Security regarding any anticipated/ upcoming visits by foreign nationals, whether the meeting is classified or not.
- Do not bring your PED into the SCIF without prior authorization.
- Be alert for phishing/ Spear-phishing

Axiologic Solutions, LLC
Annual Security Briefing

I _____, have reviewed and understand Axiologic Solutions, LLC Annual Security Briefing conducted on _____*(date)*. Topics discussed included Insider Threat, NDA's, Classification Levels, Need to Know, Personnel Security, PR's, Reportable Info, Adverse Info, Foreign Travel, Foreign & Suspicious Contacts, OPSEC, Social Networking, Security Violations, Confirming/Denying, Polygraphs, EO 13526, Information Systems, Emergency Plan, Waste & Abuse & DoD Updates.

Employee Signature_____

Last 4 of SSN# _____