2021 Security Reindoctrination Desk Reference

SAIC®

Course Modules

Module One: Personnel Security

Investigation & Clearance Process 04

Requirements for Access 05 – 06

Reporting Requirements 07 – 09

Background Investigation & Social Media 09

Adverse Information & Quick Guide

13 Adjudicative Guidelines 10 – 12

Security Violation Policy 13

Foreign Travel Reporting 13 – 14

Fraud, Waste & Abuse Poster 15

Module Two: Physical Security & Computer Security

SAIC Badges 16

Employee Badge Types 17

Clearance Indicators 17

Non–Employee Badge Types 17

Tailgating 18

Hosting a Conference or a Meeting at SAIC 18

Incoming Visits 18 – 19

Outgoing Visits 19

Foreign Nationals Visiting SAIC Facilities 19 – 20

Prohibited Items within SAIC Controlled Spaces 21 – 22

Real ID Act 22

Using Classified Systems 23

Sensitive Information & Passwords 23 – 24

Internet & Email Security 25

Computer Reporting Requirements 25

Tips for Social Media 26

Course Modules

Module Three: Information Security

Classification Management 27

Classification & Markings 27 – 31

Examples of Proper Markings 32 – 37

- Properly Marked Originally Classified Material 32
- Properly Marked Derivatively Classified Material 33
- Obsolete Declassification Markings 34
- Derivative Material based on Multiple Sources (2 Sources), Source One 35
- Derivative Material based on Multiple Sources (2 Sources), Source Two 36
- Derivative Material Bibliography for Multiple Sources 37

Information Security 38 – 40

Module Four: Counterintelligence/Insider Threat & International Security

Counterintelligence 41 – 42

Collection Methods Used by Foreign Intelligence Services 42 – 44

CI Reporting Requirements 44 – 45

Operations Security (OPSEC) 45 – 46

Insider Threat Overarching Guidance 46 – 48

The Critical Path to Insider Threat 49

Behavioral Indicators 49 – 50

Protection of Civil Rights and Liberties 50

Case Studies 51 – 52

Export Control 53

- Export Compliance 53
- International Traffic in Arms Regulations (ITAR) 53
- Export Administration Regulations (EAR) 53 – 54

Licenses & Technical Assistance Agreements (TAA) 54

International Trade Compliance Department 54

- International Trade Compliance Reminders 55

Investigation and Clearance Process

Obtain, Maintain, Terminate Clearances

"The adjudication process is the careful weighing of a number of variables, known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination." A number of factors are considered as you obtain and maintain your security clearance.

Adjudicative guidelines measure information you provide via clearance applications and standard reports, against investigative findings and resources.

Cleared individuals are responsible for submitting a Standard Form 86 (SF86), Questionnaire for National Security Positions, prior to expiration of their Background Investigation (BI) date for a Periodic Reinvestigation (PR). Not submitting an SF86 or Electronic Questionnaires for Investigations Processing (eQIP) paperwork on time adversely affects company assessment/inspection and will personally impact your clearance/access.

PR's are conducted as follows:

Confidential – 15 years

Secret – 10 years

Top Secret – 5-6 years or as directed by government requirements

Reinvestigation submittal guidelines may differ. Refer to your local Security FSO/PSO for customer specific guidance.

Background Investigation and Clearance Process

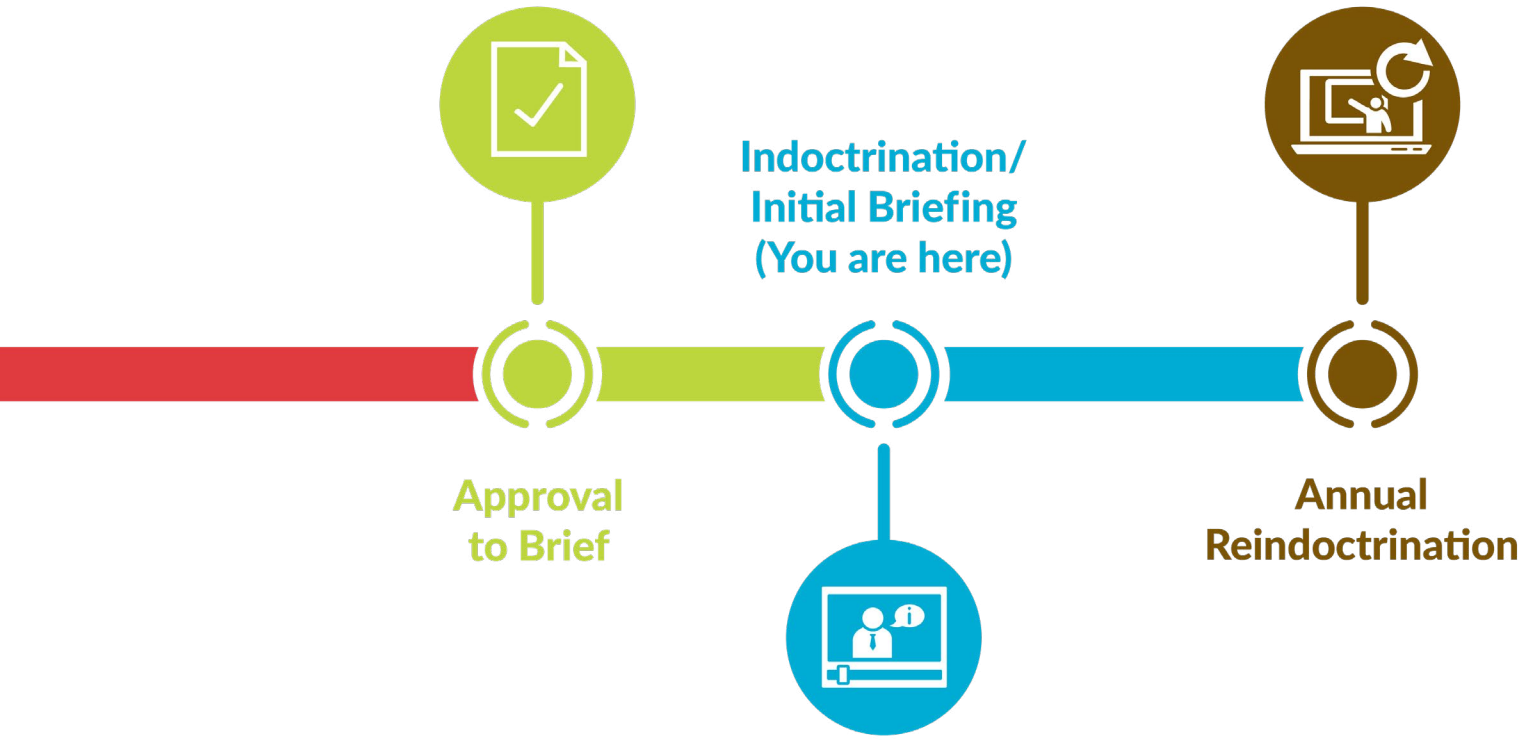
Requirements for Access

The Non–Disclosure Agreements (NDA) for the Department of Defense (DoD) (SF312), and the Intelligence Community (IC), Sensitive Compartmented Information (SCI) Nondisclosure Agreement (Form 4414), conform to the Financial Services and General Government Appropriations Act (Federal Law 112–74) and the Whistleblower Protection Enhancement Act (WPEA) (Public Law 112–199). In addition, certain customers may require other NDAs.

This strengthens protections for Federal employees who disclose evidence of waste, fraud or abuse. In addition, the WPEA modifies rules on the use of non–disclosure policies, forms or agreements (NDA's) by government agencies.

These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights or liabilities created by existing statute or Executive Order relating to:

- Classified information
- Communications to Congress
- The reporting to an Inspector General of a violation of any law, rule, regulation, or mismanagement, a gross waste of funds, an abuse of authority or a substantial and specific danger to public health or safety
- Any other whistleblower protection



Requirements for Access cont.

The following is a list of Executive Orders and Statutory Provisions, which are controlling in the case of any conflict with an agency's NDA:

- Executive Order No. 13526
- Section 7211 of Title 5, U.S. Code (governing disclosures to Congress)
- Section 1034 of Title 10, U.S. 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, U.S. Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats)
- Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential government agents)
- The statutes which protect against disclosure that may compromise national security, including sections 641, 793, 794, 798, and 952 of Title 18, U.S. Code
- Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783 (b)

Non-Disclosure Agreement

Signing an NDA is a life binding agreement between you and the U.S. Government. By signing you are:

- Prohibited from revealing classified information to an unauthorized person
- Subject to the penalties for violating U.S. Code. Penalties are severe and may include the loss of accesses, termination of position, fines and possible imprisonment.
- Required to submit information planned for public release for pre-publication review to ensure the safeguarding of sensitive and classified information

Remember

- Relationships and associations on classified contracts are not for publication and may be classified
- If you have questions or need additional guidance, contact your SAIC FSO/PSO

Need-to-Know

- Need-to-Know is an additional prerequisite for protecting classified information
- Need-to-Know is categorized as needing to know the information to be able to perform an assigned job function. If a person has a clearance and they do not have an identified Need-to-Know, you should not share information that you are protecting. This prevents unauthorized disclosure of sensitive and classified information.

Reporting Requirements

Based on the guidelines set forth in the DoD and IC for Confidential (C), Secret (S), Top Secret (TS) and Sensitive Compartmented Information (SCI), you must report the following to your SAIC FSO/PSO.

Additional contract or customer specific reporting requirements and methods for reporting may exist. Please contact your local Security FSO/PSO for additional information regarding these requirements.

Notice and Consent

In addition, SAIC and the U.S. Government and other SAIC customers or business partners may participate in certain Continuous Evaluation (CE) activities of cleared personnel for national security purposes. As a condition of holding a clearance, you consent to such monitoring of data that is relevant to U.S. national security concerns, including your eligibility to access classified and sensitive information.

Significant Life Changes

- Legal name change
- Change in marital status (including legal separation)
- Adoption
- Change in cohabitation
- Intent to marry a foreign national
- Foreign contacts
- Change in citizenship status
- Change in program/contractual support
- Customer indoctrination of additional security accesses
- Desire to no longer hold access to classified information
- Unwillingness to submit to a background investigation or polygraph examination

Foreign Travel (Pre/Post)

- All business and personal foreign trips

Foreign Contacts

- Any attempt by a foreign national to solicit sensitive/classified information or other contact that you regard as suspicious
- Close and continuing contact with foreign nationals in any capacity: in person, by telephone, over the internet, etc.
- Contact with anyone who works for or is associated with a foreign government (including a foreign embassy) or a foreign–owned organization or business
- Financial obligations to, investment in or employment with foreign nationals and companies

Reporting Requirements cont.

Computer Misuse

- Sharing passwords
- Modification, destruction or manipulation of hardware or software on government or contractor equipment

Improper Security Practices

- Inadvertent or deliberate removal of classified information
- Inadvertent or deliberate unauthorized destruction of classified information
- Inadvertent or deliberate disclosure of classified information to an unauthorized person
- Loss of classified information
- Knowledge of an unreported security violation or infraction
- Requests for classified or sensitive information through unauthorized channels
- Introduction/use of unauthorized electronics/media in a secure area

Excessive Financial Change

- Excessive indebtedness
- Liens, collections, late payments, bankruptcies, short sales, garnishments or judgments
- Financial gains (lottery, inheritance) or losses

Violation of Law/Arrest

- Litigation, arrests, court summons – ANY involvement with police (regardless of whether there is an arrest or conviction)
- Traffic citations of $300 or more
- Attempted coercion or blackmail

Emotional, Mental & Personality Disorders

Note: Strictly marital, family or grief not related to violence by you; or strictly related to adjustments from service in a military combat environment; or you were the victim of a sexual assault and consulted with a health care professional regarding an emotional or mental health condition during this period strictly in relation to the sexual assault are not reportable.

- Some prescription medications provided by a mental health professional or health care provider may be reportable
- Been declared mentally incompetent by a court or administrative agency
- Been hospitalized for a mental health condition
- Consult with your local Security POC for additional guidance on reporting
- Been ordered to consult with a mental health professional by a court or administrative agency
- Been diagnosed by a physician or other health professional with specifically listed diagnoses
- A mental health or other health condition that substantially adversely affects judgment, reliability and trustworthiness

Reporting Requirements cont.

Alcoholism and/or Alcoholism Treatment

- Arrests, treatment and/or counseling

Illegal Drug Use

- Illegal or improper use of narcotics, non–medicinal drugs, non–prescription drugs or controlled substances
- Use of prescription medication for other than its prescribed purpose
- Federal law supersedes state law. The use, possession, production, processing and distribution of marijuana is not condoned when holding a clearance and will be reported as adverse information. This includes the use of CBD oil.

Background Investigations and Social Media

The Office of the Director of National Intelligence (ODNI) released a policy for using social media for federal background investigations and adjudications for security clearances.

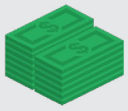
The policy does not require security investigations to consider social media information. However, it permits the collection of publicly available social media information if an agency head determines it is an appropriate investigative tool.

What is Adverse Information?

Adverse information is any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired or that his or her access to classified information clearly may not be in the best interest of national security (DoD 5220.22–M).

Reportable Information Quick Guide

A change in personal status or significant life changes, i.e., marriage, divorce, cohabitation


Financial considerations such as gains and/or losses

Drug Use

Foreign Travel and Contacts

Arrests

Unexpected Absence of employee (2hrs late or more)

Traffic Violations exceeding $300 in total fines

Emotional/Mental Health Consultation

Computer Misuse

Inadvertent or Deliberate Mishandling of Classified Information

Contact with the Media

Security Incidents

13 Adjudicative Guidelines

Adverse information may include circumstances outlined in the 13 Adjudicative Guidelines.

Allegiance to the U.S.

An individual must be of unquestioned allegiance to the U.S. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the U.S.

Example: membership in an organization that supports the overthrowing of the U.S. Government

Financial Considerations

An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Example: a history of not meeting financial obligations or an inability or unwillingness to satisfy debts

Foreign Preference

When an individual acts in such a way as to indicate a preference for a foreign country over the U.S., then he or she may be prone to provide information or make decisions that are harmful to the interests of the U.S.

Example: failure to report the possession of a foreign passport

Sexual Behavior

Sexual behavior is a security concern if it involves criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, duress or reflects lack of judgment or discretion. Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

Example: arrests for a sexual related crime

Personal Conduct

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Example: subject left previous employment due to fraud

13 Adjudicative Guidelines cont.

Foreign Influence

A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence or obligation are not citizens of the U.S. or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation or pressure.

Example: foreign financial interest or employment that may affect the individual's security responsibility

Alcohol Consumption

Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses and increase the risk of unauthorized disclosure of classified information due to carelessness.

Example: treatment for alcohol abuse

Psychological Conditions

Emotional, mental and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability or stability.

Example: information that suggests that an individual has a condition or treatment that may indicate a defect in judgment, reliability or stability

Criminal Conduct

A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Example: felony arrests, multiple misdemeanor arrests or imprisonment for over one year

Handling Protected Information

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness and ability to safeguard classified information.

Example: multiple security incidents or violations

13 Adjudicative Guidelines cont.

Use of Information Technology Services

Noncompliance with rules, procedures, guidelines or regulations pertaining to Information Technology Systems may raise security concerns about an individual's trustworthiness, willingness and ability to properly protect classified systems, networks and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation and storage of classified or sensitive information.

Example: viewing unauthorized websites

Outside Activities

Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Examples could include:

- **Service, volunteer activity or employment to a foreign country or foreign national**
- **Additional employment beyond regular job**
- **Jury Duty, court appearances, affidavits**
- **Foreign property/foreign bank accounts**
- **Political Activity as a volunteer or paid member of a staff**
- **Contact with the media and publications**
- **Dual citizenship**

Drug Involvement

Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

Example: recent drug use, illegal drug possession or drug dependence

Security Violation Policy

A security violation is an act or omission that leads to the possible or actual compromise, loss or unauthorized disclosure of classified information.

Security violations may include, but are not limited to:

- Improper security practices
- Introduction or use of unauthorized electronics in secure areas
- Classified data spills
- Mishandled classified material
- Improper marking of classified information
- Improper disclosure of classified information
- Failure to report personnel security reportable matters

SAIC has established a graduated scale of disciplinary sanctions for employee violations of security regulations or negligence.

Foreign Travel Reporting

Foreign Travel Checklist

- Notify your SAIC FSO/PSO at least 30 days in advance (when possible)
- Submit pre–foreign travel forms prior to departure
- Arrange a pre–travel meeting with your SAIC FSO/PSO
- Travel may require a defensive foreign intelligence threat and/or anti–terrorism briefing prior to travel

Remember visiting places such as a foreign embassy or foreign cruise ports are reportable.

Know–Before–You–Go

SAIC has partnered with International SOS (ISOS) to build a more robust foreign travel program.

SAIC security can provide you with a security brief that will include information on:

- Country's threat level
- In–depth security overview
- Current warnings and alerts
- Health concerns
- Available security services
- In-country assistance to include medical care, assistance with passports, currency or danger zones

Foreign Travel Reporting cont.

International SOS

Visit www.internationalsos.com

Member #: 11ByCA083835

For country specific information, sign up for alerts or download the ISOS app on your smart phone while overseas.

Travel Reminders

Be aware of your environment and the possible situations that could arise. Remember you're in a foreign country. The laws that protect you and your privacy in the U.S. do not necessarily 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
- Keep unwanted material until it can be disposed of securely
- Maintain physical control of all sensitive documents and/or mobile devices. Do not leave items that would be of value to a foreign intelligence service unattended in hotel rooms.
- Trust your instincts
- SAIC laptops may not be taken overseas without prior approval from the SAIC Cyber Assurance Team (L_CisoIntlTravel@SAIC.com)

Return Trip Follow-up Actions

- Attend a post travel meeting with your SAIC FSO/PSO
- Complete post-foreign travel forms, if required
- Report any suspicious activities and/or contacts
- Foreign Contact forms submitted as needed for close and continuous contact
    - Contacts are not only face-to-face. U.S. mail, email, chat rooms, social media sites, gaming sites, telephone, web cam, etc., are considered methods of contact.

Your PATHWAY to Reporting...

FRAUD & WASTE & ABUSE

Human Trafficking | *ABUSE OF AUTHORITY* | Bribery
SUSPECTED THREATS TO HOMELAND SECURITY
Restriction of Access to Inspector General or Congress
MISMANAGEMENT | *Leaks of Classified Information*
RETALIATION AGAINST WHISTLEBLOWERS | **Cybercrime**

3.13.2014

HOTLINE

Department of Defense

dodig.mil/hotline | 800.424.9098

MILITARY ★ CIVILIAN ★ CONTRACTOR

Physical Security

These items, used together, provide layers of protection called Security–In–Depth. They are designed to work together so that if one item were to fail, the next item could detect, delay and report the issue.

- Perimeter entry controls
- SAIC picture badges
- Intrusion Detection Systems (Alarms)
- Guards
- Prohibited item controls
- Escorting
  - Receive an escort briefing from your SAIC FSO/PSO to understand your roles and responsibilities
- Entry/exit inspections
- Employees are responsible for securing information in their possession and their workspace
  - Part of securing your workspace means complying with physical security requirements

SAIC Badges

Purpose

The primary purpose for wearing an SAIC badge in our facilities is to provide "positive circulation control" and physical access to protect classified information and SAIC proprietary data.

Display your badge above the waist in plain sight while in the facility.

Ask for a Badge

If you don't see a badge on a person, it is your right and obligation as an employee to ask the person to produce one. If they do not have a badge, escort them to the main lobby to sign in and receive a badge.

Remove and Protect your Badge when Leaving the Facility

- Store your badge in a safe place, out of plain sight
- Think Operations Security (OPSEC). Even your lanyard could give away too much information.
- Don't give people the opportunity to see your credentials and identify yourself as an employee. You become a target for solicitation and possible association concerns.

Lost/Misplaced Badge

- Report to SAIC security immediately

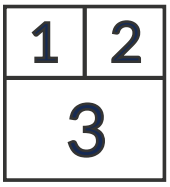
Employee Badge Types

Uncleared Employee

Foreign National

Permanent Resident

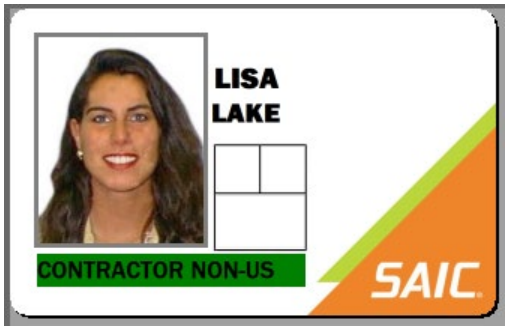
Clearance Indicators



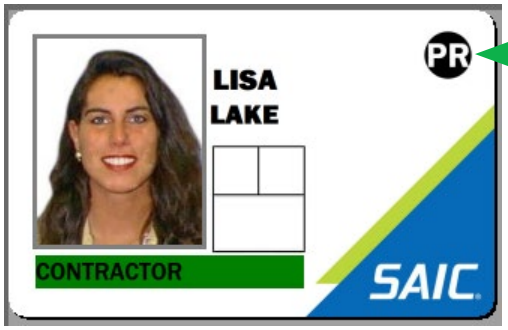
The boxes next to the picture represent the clearance level

- Secret represented by a one (1)
- Top Secret represented by a two (2)
- SCI represented by a three (3)

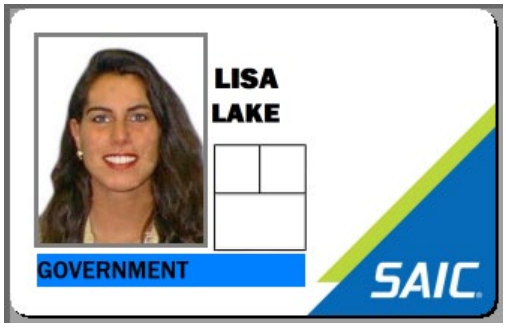
Non–Employee Badge Types



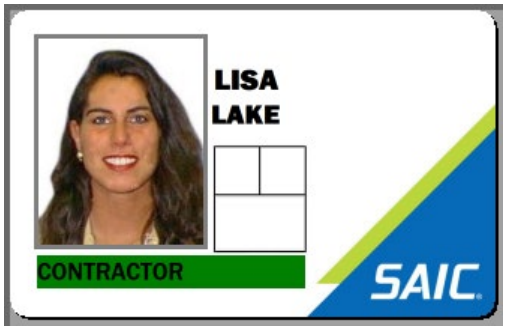
Foreign National Contractor



Permanent Resident Contractor



Government Uncleared



Contractor Uncleared

Tailgating

Employees and visitors shall wear the SAIC badge visibly, above the waist at all times while on company property and shall swipe their access badge at all badge readers before entry into non-public space, as "tailgating" is not permitted.

Hosting a Conference or a Meeting at SAIC

All visitors are the responsibility of their SAIC host while in our facilities. You as "the host" ensure:

- You know who is attending
- Visitors sign in and receive proper SAIC badges
- You know the classification level for the conference/meeting
  - Unclassified
  - TS/SCI
  - DoD Collateral
- Do they have the proper clearance and has it been verified by SAIC security?
  - Do they have a Need–to–Know for the information? If an SAIC employee is not releasing the information, has the Need–to–Know been approved by the government technical point of contact?
- You know what classified materials (if any) are being brought in/carried out
  - Has this been coordinated with SAIC security?
- You know what network will be required to support the conference/meeting
- You provide opening remarks
  - Set the level of the meeting
  - Include a brief "Emergency Procedures" statement, exit locations and procedures to secure classified information if time permits and does not threaten personal safety

Incoming Visits

Notify security if you are expecting a visitor for a classified area.

Please have visitors provide the following information.

DoD and SCI Requires:

- Date(s) of visit
- Purpose of visit
- Technical Point of Contact (SAIC)
- Clearance/access level

Incoming Visits cont.

- Name
- SSN
- Date of birth
- Place of birth
- Citizenship
- Date of clearance
- Clearance granting agency

Visit certifications should be received 48 hours prior to visit (if possible).

Outgoing Visits

If you are visiting a customer or industry partner facility and need your clearance or accesses sent, please include the following information on your visit request:

- Date(s) of visit
- Purpose of visit
- Technical Point of Contact/phone number
- Clearance/access level required for meeting
- Corporation name and location/government agency to be visited
- Security Points of Contact/phone numbers

Allow three days advanced notice to make sure that the request is processed. It is the employee's responsibility to ensure receipt of VAR at their destination.

Foreign Nationals Visiting SAIC Facilities

Do you have foreign nationals visiting and are all the approvals in place, regardless of classification levels?

- Coordinate in advance (at least 5 days). Approvals are required within SAIC and in most cases require government security approval.
- Complete and submit the Foreign Visitor Request Form located on ISSAIC
- Review the Technology Control Plan (TCP) located on ISSAIC
- Make sure you know what can/cannot be discussed
  - Applies to meetings and conversations/discussions both at SAIC and non SAIC locations
  - There are restrictions on technical discussions and access to technical materials (even at the unclassified level)
  - SAIC employees **may not** have technical discussions with the foreign national (unless approved Government authorization is in place)
  - SAIC employees **may not** do a technical presentation on behalf of the government (unless approved Government authorization is in place)
  - If no Government authorization is in place, SAIC employees cannot share controlled export data directly with foreign nationals

Foreign Nationals Visiting SAIC Facilities cont.

- Foreign nationals badges are marked with an orange triangle for easy identification
- Foreign nationals must be escorted at all times at a 1:3 ratio
- Foreign nationals showing up unannounced is an intelligence collection method and must be reported to our government security customer.
    - Unannounced or last minute substitutions of foreign nationals will not be granted access to the facility

Most visitors are here for a legitimate purpose, but the sheer volume of visitors makes it difficult to detect those who come with ulterior motives.

- Foreign delegation visitors to cleared contractors are one of the most frequent methods of operation used to target the U.S. defense industry
- Any line of questioning concerning your contract information should be viewed as suspicious behavior
- Even if an appropriate authority grants a foreign visitor access to classified U.S. information, that visitor is not entitled to classified information unless he/she has a Need–to–Know that has been communicated and verified in advance of the visit
- Some of our government sponsors, when given adequate time, can assist with identifying the risk to the cleared company, technology or our personnel

Gathering Techniques Used by Foreign Intelligence

Peppering

- Visitors asking the same question in different styles or one visitor asking the same question 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 and Conquer

- Visitors take a U.S. person into different areas to discuss issues in order to deprive 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 and 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 and 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

Security Countermeasures for Foreign Visits

- Ensure visits are pre-coordinated
- Ensure proper circulation control – only allow access to facility areas involved in the visit
- Ensure proper escort to foreign national ratio 1:3
  - Escorts should conduct a walk-through of the facility prior to the visitor arriving to ensure they will not have audible or visible unauthorized access. Escorts need to be with visitors at all times.
  - Ensure escorts are briefed of protection requirements
- Do not allow discussions/questions beyond the scope of meeting as annotated on the approved visit request
- Do not permit any cameras/recording devices to include cell phones during foreign national visits (regardless of meeting level)

Tips for Responding to Suspicious Questions

- Prior to visit, all personnel working with the delegation are made aware of what can and cannot be discussed
- If the delegation attempts to make additional contacts with escorts and/or speakers, make sure they understand to keep the discussions to an agreed-upon topic and information

Contact your SAIC FSO/PSO with questions regarding hosting meetings or the visit certification process.

Prohibited Items within SAIC Controlled Areas

There are many different controlled spaces within SAIC facilities, i.e., restricted areas, closed areas, Sensitive Compartmented Information Facilities (SCIF's), Special Access Program Facilities (SAPF's). It is your responsibility to know the rules for the facility/space you are working in and what can and cannot be introduced to those areas. Contact your SAIC FSO/PSO if you are unsure whether a specific item is prohibited.

Prohibited items don't just apply to SAIC controlled areas.
What is prohibited in one facility may not be in another.

Prohibited Items (but not limited to)

- Firearms, explosives, drugs or any items in violation of the law
- Personally owned computers, peripheral devices, media, software
- Photographic, video and audio recording equipment
- Cell phones, modems, two-way transmitting equipment (IR/RF)
- Satellite radios
- Government equipment is prohibited unless approved by security
- Medical Portable Electronic Devices (MPED's)

Prohibited Items within SAIC Controlled Areas cont.

- As technology continues to evolve, more and more healthcare providers prescribe the use of MPED's. While some of these devices may be required for a temporary use to monitor or track conditions, some may be needed longer.

- Some of the devices may even utilize technologies that have been prohibited inside of a controlled space. Our customers understand the need for such devices. If you are prescribed one of these devices please contact your SAIC FSO/PSO. They will help coordinate any approvals necessary as well as provide any feedback regarding potential mitigation of some of those prohibited capabilities.

REAL ID Act

The REAL ID Act is a federal law that creates national standards for state–issued driver's licenses and requires federal agencies (and contractors) to apply the new rules for individuals entering their facilities.

SAIC can Mitigate Potential Issues with this Regulation

- The SAIC host can notify their visitors of this regulation. If the visitor has a driver's license from a non–compliant state, the visitor should be informed that they should bring a second form of identification.
- If the visitor does not have an accepted form of secondary identification, the SAIC host can verify, in–person, the identity of the individual before they are allowed to enter the facility. This is only to validate the visitor's identity. Visit certifications must be in place before admittance to meetings.

Accepted Form of Secondary Identification

- U.S. & Foreign Passports
- U.S. Military Identification Card
- U.S. Military & DoD Common Access Cards (CAC)
- U.S. Federal Government Identification Card & Credentials
- U.S. Congressional Identification Cards

For real-time updates please see https://www.dhs.gov/real-id

Using Classified Systems

User accounts are regularly validated and unused accounts may be disabled without notice.

Users of a classified system require:

- Proper access and clearance level
- All applicable caveat briefings
- Need-to-Know

Classified systems are accredited for specific purposes and are not authorized for personal use including but not limited to:

- Mp3s
- Games
- Personal software/hardware
- Entertainment

Sensitive Information and Passwords

Protect customer data, SAIC data, Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI) such as For Official Use Only (FOUO).

- Do not share SAIC business or customer information on social networking sites, blogs and websites
- Encrypt sensitive data

Passwords

According to SI-POL1-09, passwords must be at least eight characters long and must include at least three of the four attributes: upper case letter, lower case letter, number and special character (e.g., _,$,%,@,#). Passwords should not consist of common terms or other easily guessed or derived word combinations.

- Do not use dictionary words, names or birth dates as these can be presumed in seconds

Consider Using a Phrase Rather Than a Single Word

- A phrase (i.e. more than one word) usually results in a longer, more complex password and therefore, more secure than a password formed from a word
- Phrases also help ensure your password is memorable

Do Not Write Down your Password – Commit it to Memory

- Never share your password with anyone
- If passwords are shared, you can be held responsible for any loss, damage or misconduct that arises from its use
- Never log on and let others use your account
- Logout of your system if you are leaving for the day
- Lock your computer screen when you are beyond line of sight

Media Handling

- **Best practice**: Once media touches a classified system, treat it as classified at the level of that system
- **Never** introduce classified media to a system not approved for the level, caveat or Need-to-Know of the data
- **Always** mark media to appropriate classification level and bring to Document Control
- There are **no** "Working Papers" for media
- **All** media must be **scanned** for malicious code before being introduced to the system
- Ensure media is protected to include **clearance, caveat** and **Need–to–Know** — to include "waste media"

Assured File Transfer

- The process of moving data from a lower classified system to a higher classification system, from High-to-Low, or systems of the same classification.
- **Assured File Transfer is strictly prohibited without written approval from your SAIC ISSM/PSO**
- If not authorized, **printing** is the best alternative

Hardware & Software Requirements

- Any transportation of classified systems from the facility must be approved by an SAIC ISSM/PSO
- Any introduction of customer classified systems to the facility must be approved by an SAIC ISSM/PSO
- All hardware or software modifications must be taken to the local SAIC ISSM/PSO prior to installation for approval
- All system maintenance or repairs must be conducted by a privileged user or SAIC escorted technician and logged

Spills

What is Spillage?

- Spillage is a situation where there is a concern that classified information may have been introduced to a system not approved for the classification, caveat or Need–to–Know for the information

Some examples of spillage involving computer systems:

- Classified information discovered on an unclassified or otherwise unapproved system (email, documents, PowerPoint presentations)
- Higher level classified information on a system approved at a lower classification level (TS on a Secret system)

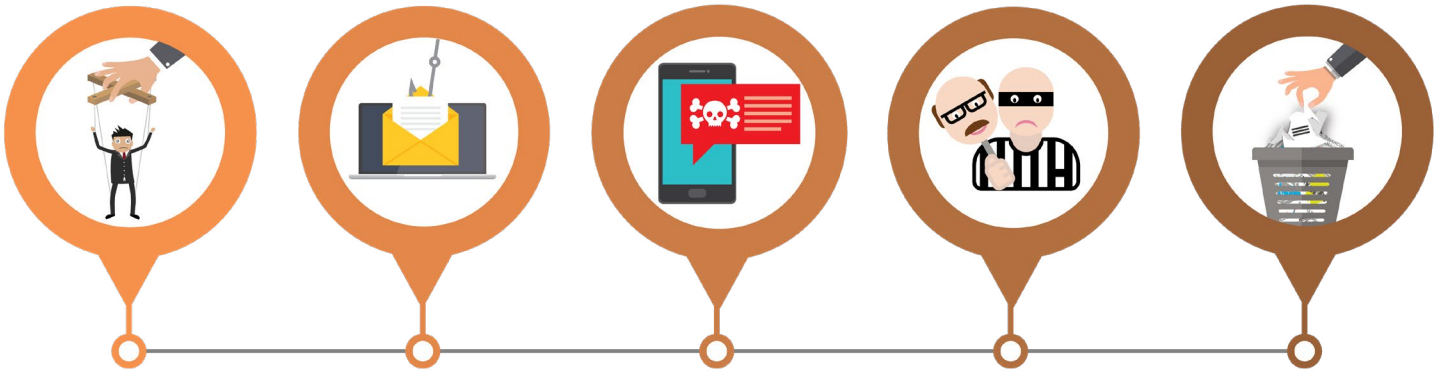
Contact your SAIC FSO/PSO/ISSM if you believe a spill has occurred, or if you have any questions.

Internet & Email Security

Beware of Scams

Criminals and hackers constantly come up with new schemes designed to compromise computers, valuable information (personal, financial, etc.) and/or passwords. This is often referred to as "social engineering."

Some tactics include:



Social Engineering

A non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

Phishing

Deceptive emails, text, posts on social networking sites or pop-ups. They often ask you to reply with personal info, click on a link, or open a file.

Vishing

Similar to Phishing, but focused on the use of telephones to attempt to scam the user into surrendering private information that will be used for identity theft.

Impersonation

When attackers pose as someone in authority, or an IT representative, to obtain information or direct access to systems.

Dumpster Diving

Going through trash to obtain valuable information for targeted attacks.

Computer Reporting Requirements:

Any of the following activities must be reported immediately:

01 **Procedural Deviations**

02 **Malicious Activity**

03 **Discovery of Vulnerabilities**

04 **Suspected or Actual Compromise**

Some examples include:

- Malfunctioning system security
- Unsecured media or documents
- Viruses on classified systems
- Unauthorized access

When in doubt, report it!

Tips for Social Media

Social networking sites are a great way to connect and share information, but with the amount of visitors these sites attract this makes them extremely vulnerable to cyber criminals. Some countermeasures while using social networking sites to keep in mind are:

- Only establish and maintain connection with people you know and trust. Review your connections often.
- Assume that anyone can see any information about your activities and personal life that you post and share
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing setting can expose your personal data
- Everything posted on a social networking site is permanent. Even if you can delete your account, anyone on the Internet can easily print photos, text or save images and videos.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points
- Limit how much information you reveal in your profile. Clearance information, poly types and dates, company details, customers and locations you support, etc., should not be listed.
- Use your personal email address for social media accounts or profiles. Your company email address should not be used.
- Use caution when clicking links that are received in messages or posts
- Type the address of the social networking site directly into your browser or use your personal bookmarks. If you click a link to the intended site through email or another website, you might be entering your account name and password into a fake site where personal information could be stolen.

Individuals often do not take into consideration the amount of information they are posting to social networking sites because there is a false sense of security since you are not face-to-face:

- Internet provides a sense of anonymity
- The information is intended for their friends to read, forgetting that it is out there for others to see
- They want to offer insights to impress potential friends or associates

SAIC employees should not identify their employment status, location, salary, clearance, travel itineraries, customers, etc., and should not use company email addresses.

Classification Management

Why do we Portion Mark?

- To identify and protect classified information
- To facilitate the sharing of information among agencies
- To distinguish different classification levels within a document
- To aid in future review and release of documents
- Executive Order 13526 and ODNI CAPCO document mandates that ALL classified material be portion marked

What is Portion Marking?

Banner markings (headers and footers) and portion markings include:

- Classification Levels:
  - Unclassified (U)
  - Confidential (C)
  - Secret (S)
  - Top Secret (TS)
- SCI Control Systems:
  - Special Intelligence (SI)
  - Talent Keyhole (TK)
  - Reserve (RSV)
  - HUMINT (HCS–O/P)
- Dissemination Controls:
  - NOFORN: Not releasable to Foreign Nationals
  - REL TO: ____ Releasable to: ____
  - ORCON: Originator Controlled Dissemination
  - PROPIN: Proprietary Information
  - FOUO: For Official Use Only

The classification MUST be fully spelled out in the banner/headers and footers; control systems and disseminations may be abbreviated.

Classification and Markings

Executive Order 13526 establishes the criteria for classification and protection of National Security Information.

An Original Classification Authority (OCA) is a government official who is designated in writing by the U.S. Government to make classification determinations. Their function is to establish classification guidelines, reasons, durations and declassification exemptions.

Classification and Markings cont.

A derivative classifier incorporates, paraphrases, restates or generates a new form of information that is already classified.

SAIC Employees Involved in Generating Classified Material are Derivative Classifiers

As a Derivative Classifier, you are to self–identify and carry forward instructions for classification and markings from sources, customer instructions and/or classification guidance. Never originally apply classification markings, downgrade classified information, guess or assume classification levels, provide "subject matter expertise" or classification guidance to any source unless authorized by an OCA or classification guide.

Per the Under Secretary of Defense for Intelligence (USDI) Memorandum – Derivative Classification Training dated 31, Jan 2019: Derivative Classification Training must now be completed on an annual basis.

Derivative Classifiers

- Self-identify on derivatively created classified materials
- Carry forward instructions on classification and markings from sources, customer instructions and/or classification guides
- Identify source(s) on the "Derived From" line
- Challenge/seek clarification for incorrect/incomplete markings/ instructions on derivatively classified materials
  - Challenges are directed to an OCA with jurisdiction over the information
  - A formal challenge must be completed in writing
  - No retribution is taken against any authorized holders bringing such a challenge in good faith
  - The agency shall provide an initial written response to a challenge within 60 days
  - Informally questioning the classification status of particular information is encouraged as a means of holding down the number of formal challenges

Difference Between OCA and Derivative Classifier

- For derivative classifiers, a reason code is not required
- OCA identification is replaced with derivative classification authority identification

Required Identification Markings for All Materials, to Include Media

- Classification banner marking
- Portion marking
- Date
- Title

Required Identification Markings for All Materials, to Include Media cont.

- Identification marking
- Classified By (original or derivative)
- Reason (required only for original classified material)
- Derived from (required only for derivatively classified materials)
- Declassification instructions
- Email, email attachments

Generation of Working Papers (where applicable)

- Writing classified information on a sheet of paper derived from a final document or based on an in-house classified discussion
- Printing the classified material from an authorized Information System approved printer
- Making an approved photocopy on authorized equipment of controlled final material (the copy may be considered a working paper)

Working Papers Required Markings (where applicable)

- Follow your local requirements when dealing with overall classification (to include caveats and/or dissemination controls if applicable)
- Date created
  - Include name of creator
- The annotation "Working Papers" preferably applied to all pages
- In some cases they must be controlled and marked in the same manner as a finished document

Working Papers are different in that they remain Working Papers for 180 days for Confidential and Secret and 30 days, per SAIC guidelines, for Top Secret from date of origination. After this time period, they are either destroyed or placed into the accountability system, depending on facility requirements.

Caveats (Collateral)

- RD: Restricted Data (DoE, AEA 1954 as amended)
- FRD: Formerly Restricted Data (DoE, AEA 1954 as amended)
- CNWDI: Critical Nuclear Weapon Design Information (DoD)
- NATO: North Atlantic Treaty Organization (Central U.S. Registry; Annual Briefing Requirement, monitored by local FSO)
- NATO Abbreviations/Levels: Confidential (NC), Secret (NS) and Top Secret (COSMIC) (CTS); NATO containing Restricted Data/Formerly Restricted Data (ATOMAL) according to level are abbreviated (NCA), (NSA), (CTSA)
- FGI: Foreign Government Information; portion mark (country// classification), e.g., (UK-C) if the identity of the country of origin must be concealed, portion marking is (FGI-C)

Dissemination Controls

- NOFORN (NF) Not Releasable to Foreign Nationals
- Authorized for intelligence information only
- When applied within collateral information, verify its appropriate use
- When NOFORN and REL TO are in the same material, NOFORN trumps REL TO in the overall banner marking
- RELEASABLE TO (REL TO):
  - Categories of REL TO are commonly referred to as
  - FIVE EYES (FVEY) = USA/AUS/CAN/GBR/NZL
  - List USA first on all REL TO materials

Control markings used in the banner and portions that identify the expansion or limitation on the distribution of information.

Dissemination Controls do not require briefings.

Prohibitions

- Avoid over-classification
- Consult Government Contracting Activity (GCA) or the Security Classification Guidance (SCG) when in doubt
- Avoid "stripping" classified to create unclassified materials (without GCA or government review)
- Avoid implied "unclassified" information in order to avoid classification

Limitations

- Must determine in writing that reclassification of the information is necessary in the interest of national security
- Reasonably recoverable
- Reported to Information Security Oversight Officer (ISOO) within 30 days

Reclassified information must be appropriately marked and safeguarded

Sanctions

Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information or other sanctions in accordance with applicable law and agency regulation.

When a document reaches its declassification date, this does not automatically make the document unclassified and ready for public release. Determinations for re-classification are made at the OCA level. Refer all questions to your customer program office.

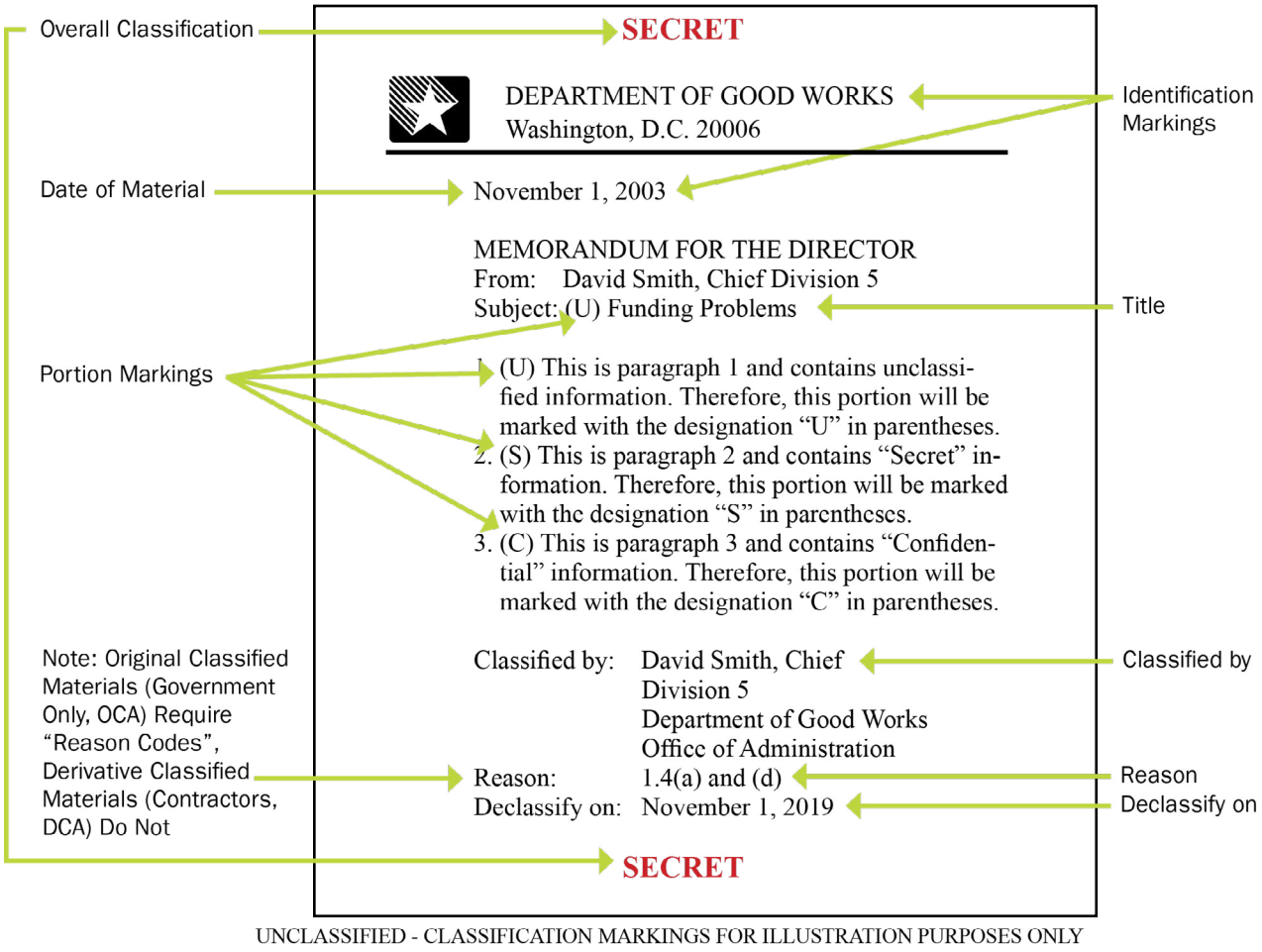
There are penalties for violating inappropriate handling and disclosure of classified information.

Marking Originally Classified Information

The overall process for properly marking a document requires the classifier to:

- Identify the classification level of each portion contained in the document
- Determine the overall classification of the document
- Identify the original classification authority on the "Classified by" line
- Identify the reason for classification
- Every classified document shall show on the first page, title page or front cover, the "originating agency and office and date of the documents origin"
- Annotate the declassification instructions on the "Declassify on" line (if applicable)

Ex. 1: Properly Marked Originally Classified Material



01 Identify the classification level of each portion contained in the document

02 Determine the overall classification of the document

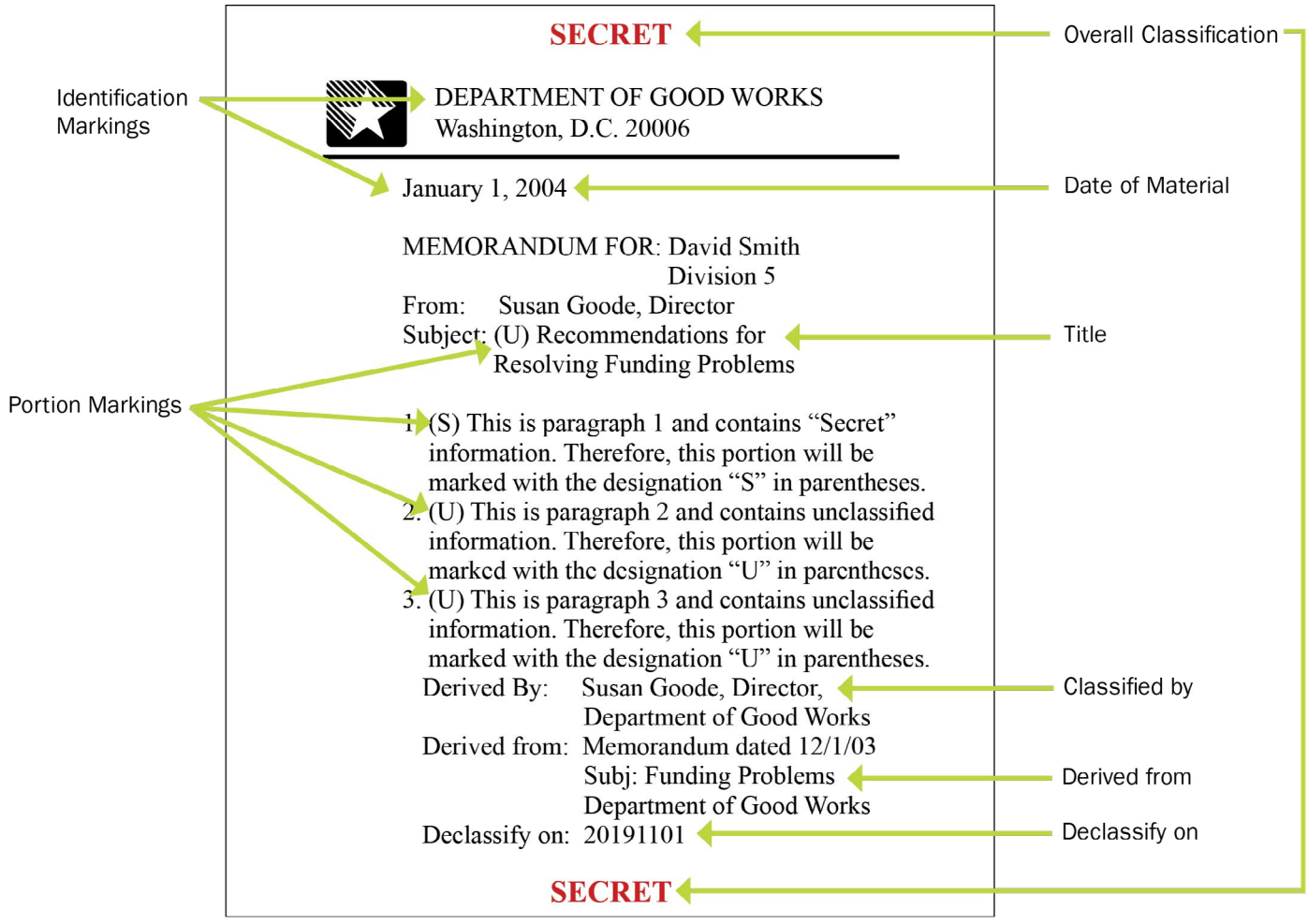
03 Identify the original classification authority on the "Classified by" line

04 Identify the reason for classification

05 Every classified document shall show on the first page, title page or front cover, the "originating agency and office and date of the documents origin"

06 Annotate the declassification instructions on the "Declassify on" line (if applicable)

Ex. 2: Properly Marked Derivatively Classified Material



UNCLASSIFIED - CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

01 Identify the classification level of each portion contained in the document

02 Determine the overall classification of the document

03 Identify the original classification authority on the "Classified by" line

04 Identify the source for derivative classification, or list "Multiple Sources" and attach the source list to the material

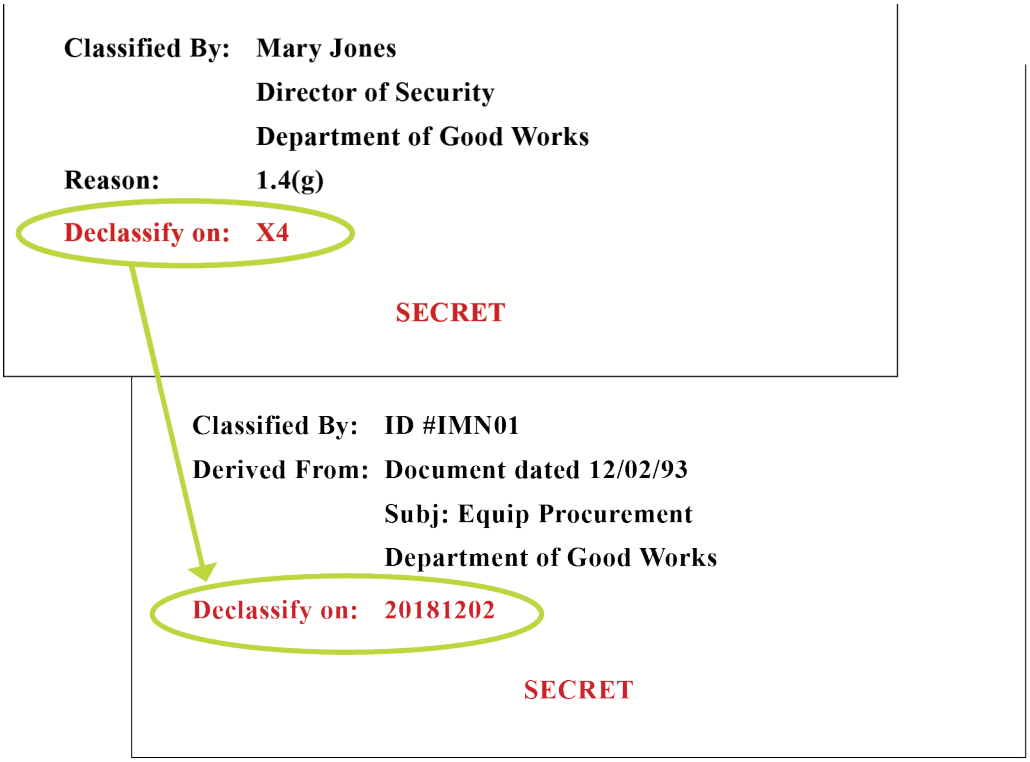
05 The overall classification, to include caveats and dissemination controls, as well as any required caveat disclaimers must also be include on these pages. This applies to all material types, including media.

06 Annotate the declassification instructions on the "Declassify on" line (if applicable)

Ex. 3: Obsolete Declassification Marking

When a document is classified derivatively either from a source document(s) of a classification guide that contains one of the following obsolete declassification instructions, "Originating Agency's Determination Required," "OADR," "Manual Review," "MR," or any of the exemption markings

"X1, X2, X3, X4, X5, X6, X7, and X8," the derivative document's date or event to be placed in the "Declassify on" line. If no source date is available, then use the current date.



UNCLASSIFIED - CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Ex. 3.1: Derivative Material Based on Multiple Sources (2 Sources), Source 1

Source 1: Original Material

Declassification instructions list X4, out of use effective 22 September 2003

SECRET//NOFORN

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

September 1, 2007

MEMORANDUM FOR THE DIRECTOR
From: Mary Jones
Subject: (U) Security Equipment Procurement

1. (S//RELTO USA, CAN) This is paragraph 1 and contains "Secret" information releasable to the United States and Canada. Therefore, this portion will be marked with the designation "S//RELTO USA, CAN" in parentheses.

Classified by: Mary Jones
Director of Security
Reason: 1.4(g)
Declassify on: X4

SECRET//NOFORN

IAW EO 13526 Declass Calculation:

- Source Date + 25 Years
- No Source Date = Date of Derivative Material + 25 Years

In this case, this is an original source dated 1 September 2007.

Therefore, declassification for 1 September 2007 + 25 = 20320901

If this original material were not dated, you would apply 25 years post the date of your derivative material's creation for declass.

UNCLASSIFIED - CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Ex. 3.2 Derivative Material Based on Multiple Sources (2 Sources), Source 2

Source 2: Derivative Material

Declassification instructions list OADR, out of use effective 14 October 1995

IAW EO 13526 Declass Calculation

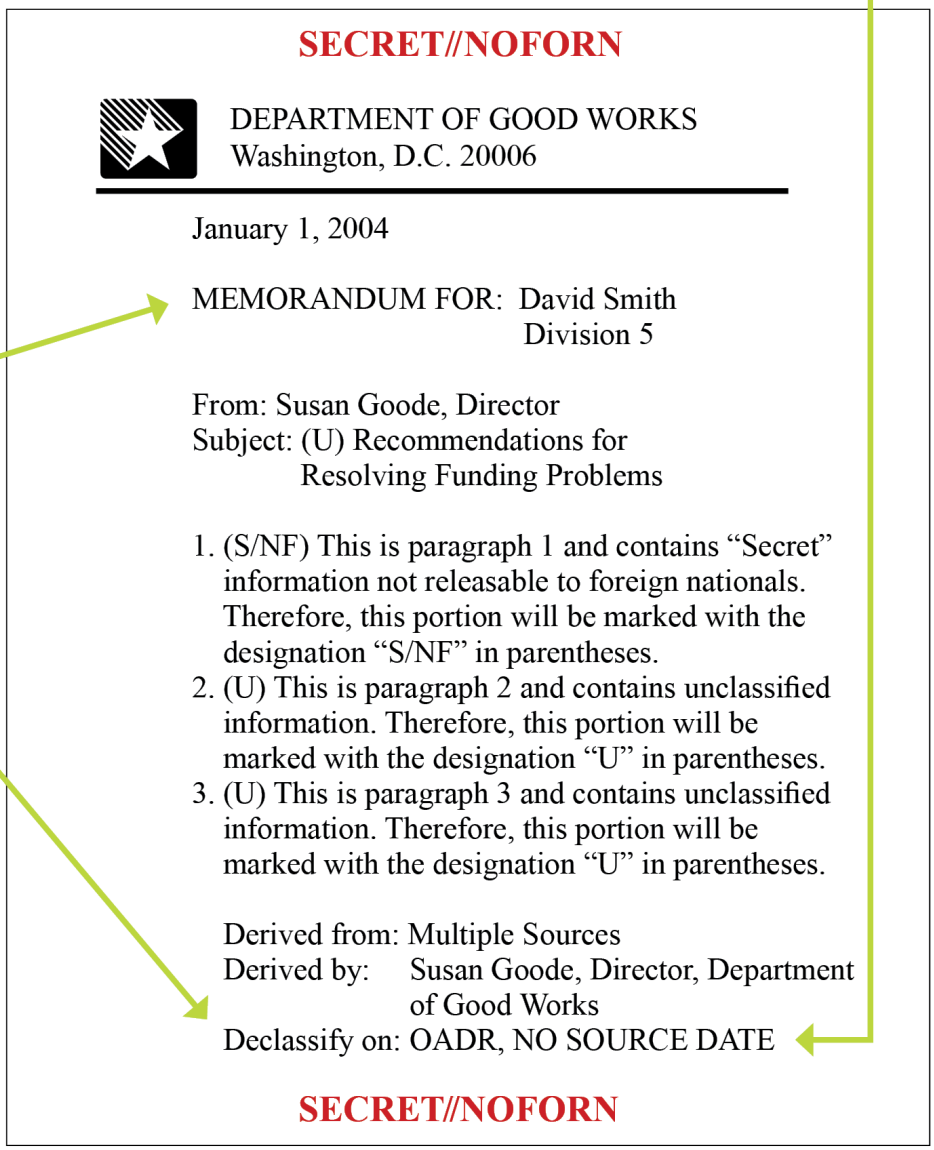
- Source Date + 25 Years
- No Source Date = Date of Derivative Material + 25 Years

In this case, no source date is listed for this derivative material generated from another source.

Therefore, Declassification is 1 January 2004 + 25 = 20290101

If this derivative material were not dated, you would apply 25 years post the date of your derivative material's creation.

Source 2 is based on multiple sources. When citing this source in your derivative material's bibliography, provide the source date, author, date, and subject of this material (do not list "multiple sources" as one of your sources).



SECRET//NOFORN

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

January 1, 2004

MEMORANDUM FOR: David Smith
Division 5

From: Susan Goode, Director
Subject: (U) Recommendations for
Resolving Funding Problems

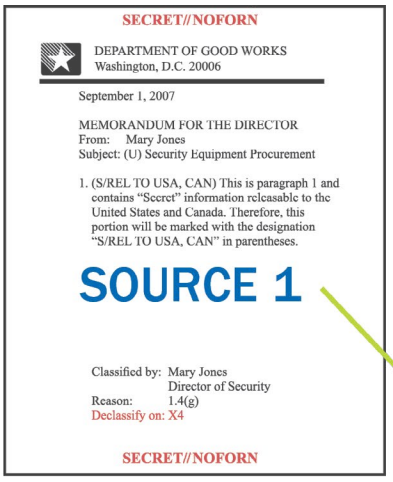
1. (S/NF) This is paragraph 1 and contains "Secret" information not releasable to foreign nationals. Therefore, this portion will be marked with the designation "S/NF" in parentheses.
2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.
3. (U) This is paragraph 3 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Multiple Sources
Derived by: Susan Goode, Director, Department of Good Works
Declassify on: OADR, NO SOURCE DATE

SECRET//NOFORN

UNCLASSIFIED - CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Ex. 3.3: Derivative Material Bibliography for Multiple Sources



SECRET//NOFORN

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

September 1, 2007

MEMORANDUM FOR THE DIRECTOR
From: Mary Jones
Subject: (U) Security Equipment Procurement

1. (S/REL TO USA, CAN) This is paragraph 1 and contains "Secret" information releasable to the United States and Canada. Therefore, this portion will be marked with the designation "S/REL TO USA, CAN" in parentheses.

SOURCE 1

Classified by: Mary Jones
Director of Security
Reason: 1.4(g)
Declassify on: X4

SECRET//NOFORN

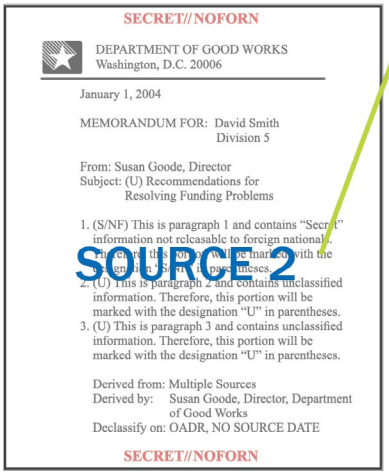
Include Material Date, OCA or DCA Name, Title/Organization/Source Title

Although Source 2 was based on "multiple sources", identify the source itself for the derivative source list (sources must be traceable, avoid listing multiple sources in perpetuity).

Derived From: Multiple Sources

Source 1: Memo of 1 September 2007
Mary Jones, Director of Security
Department of Good Works
Subject: Security Equipment Procurement (U)

Source 2: Memo of 1 January 2004
Susan Goode, Director
Department of Good Works
Subject: Recommendations for Resolving Funding Problems (U)



SECRET//NOFORN

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

January 1, 2004

MEMORANDUM FOR: David Smith
Division 5

From: Susan Goode, Director
Subject: (U) Recommendations for Resolving Funding Problems

1. (S/NF) This is paragraph 1 and contains "Secret" information not releasable to foreign nationals. Therefore, this portion will be marked with the designation "S/NF" in parentheses.
2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.
3. (U) This is paragraph 3 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Multiple Sources
Derived by: Susan Goode, Director, Department of Good Works
Declassify on: OADR, NO SOURCE DATE

SECRET//NOFORN

SOURCE 2

UNCLASSIFIED - CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Information Security

Marking Information

The overall process for properly marking a document requires the classifier to:

- Ensure all documents and emails are marked correctly
- Use appropriate cover sheets:
  - SAIC generated for internal use
  - Government issued for deliverables

Storing Materials

Store materials appropriately based on the approved storage requirements for your facility.

Handling

You are responsible for handling information appropriately. Review all material before removing from a controlled area and follow the correct handling procedures for your facility.

Transmitting/Transporting Classified Material

Working with classified materials carries significant responsibilities. It is your responsibility to keep it safe from compromise. This is especially important when you need to electronically transmit or physically transport classified material.

Classified material must be electronically transmitted and/or physically transported via the approved methods in place at your facility based on the government's guidance and policy.

Guidance will vary per classification level and agency. Contact your local FSO/PSO for procedural and policy guidance.

Pre-Publication Review

Depending on the government sponsor you support, written and oral materials to be published or presented may need to be submitted for approval to the government for review prior to release.

- Résumés
  - Can list TS/SCI with polygraph
- Speeches, articles, white papers
- Web pages, web sites or blogs
- Biography
- Books, memoirs, literature (including fiction)

Plan in advance. Most government agencies have up to 30 days to respond to your request with an approval or notification of a new deadline.

Ask your SAIC FSO/PSO for assistance with pre-publication reviews and the process that your government sponsor requires.

Information Security cont.

Public Disclosure

Never confirm, deny, validate or clarify information appearing in open source publications: TV, media or the Internet.Reproduction

Never leave documents lying around in the open copy/print or fax areas. This is a common way for information to be compromised by others. Collect documents from the printer as soon as they print and don't forget to pick up the originals from the copier or fax machine.

Shared Conference Rooms

Don't leave sensitive information behind. Remove all information from flip charts and wipe down the whiteboards.

Destruction

- Never throw sensitive information in the trash – information is commonly leaked this way through "dumpster diving"
- Ensure all classified information is securely disposed of by approved methods for your facility
- Contact your SAIC FSO/PSO on destruction procedures
- At the end of a contract, information is either destroyed or returned to the customer

Telephone Awareness

- Do not "talk around" classified information on unsecure lines
- Be cognizant of discussions taking place around you while using an unsecure line
- Report any suspicious solicitations, head hunters, etc.
- Be wary of phishing scams

Report these instances to your SAIC FSO/PSO.

Remember

- Neither confirm nor deny the validity of any classified or SAIC proprietary information that appears in open source publications
- Open publication of classified information does not declassify the information. Only the government is authorized to declassify information.
- Please notify your SAIC FSO/PSO if you see something in the public arena that you believe is classified
- Protecting both classified and unclassified information is important
- Proprietary information and PII is unclassified information that warrants protection
- Publication of classified information does not necessarily mean it has been declassified. Classified information leaked to the media in the past has caused grave damage to national security. Prior to declassifying

Information Security cont.

information, formal approval and authorization must be received through proper channels from the government.

Ensure

- Material is never left unsecured or unattended (follow local site procedures)
- Work area is appropriately approved and properly prepared for classified work
- Co–workers and visitors have appropriate clearance level and Need–to–Know
- Mark classified material appropriately
  - Never save, view, insert, produce or transmit via an unclassified system
  - Stored appropriately when not in use
- Combinations to containers are protected at same level as the information they are protecting
- Use caution when revealing details regarding program names, technology, mission, locations, cost and research and development activities. Compilation of unclassified facts could make the information classified.
- When hand-carrying classified, ensure that you have been properly briefed, issued a courier card/letter if necessary and your materials are secured appropriately

What is Counterintelligence (CI)?

Counterintelligence is about identifying threats and developing strategies to mitigate those threats. Counterintelligence consists of the actions we take to counter adversary intelligence, espionage and sabotage efforts.

E.O. 12333 – U.S. Intelligence Activities

Elements of the IC are authorized to: collect, retain or disseminate information regarding U.S. persons by the least intrusive techniques feasible. The U.S. Government has a solemn obligation and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all the U.S. persons, including freedoms, civil liberties and privacy rights guaranteed by Federal Law.

Threats

The best way to counter threats is to know the targets, know your adversaries, know how to protect and report information and always report any suspicious activity or attempts to obtain information.

External Threats come from Many Places

- Foreign Intelligence Service(s) (FIS)
  - External threats in the form of FIS can come from not only what we consider non–ally countries. They can come from our allies as well.
- Foreign and Domestic Industry Competitors
  - Industry competitors (industrial espionage) seek to gain our information to gain a competitive edge
- Criminal, Activist and Terrorist Organizations
  - Criminals/activists and terrorist organizations often look to obtain our information in order to further a cause vs. gain an edge

What is Counterintelligence (CI) cont.

Defensive Measures to Deny Adversaries any Information

You must identify, control and protect unclassified information related to sensitive activities to reduce vulnerabilities to our information.

- Counterintelligence protects classified and sensitive information
- Do not disclose classified information or unclassified information (especially related to classified contracts)
- Do not disclose export controlled information or technical data protected under the International Traffic in Arms Regulations (ITAR)
- Be aware of strangers asking for information not related to their job scope
- Reduce your profile as a member of the IC and/or DoD

Collection Methods Used by Foreign Intelligence Services

Methods of Contact are the approach used to connect the foreign actor to the targeted individual, information, network or technology in order for the foreign actor to execute the Methods of Operation.

Collection Methods Used by Foreign Intelligence Services Cont.

Methods of Operation are a distinct pattern or method of procedure thought to be characteristic of or habitually followed by an individual or an organization involved in criminal or intelligence activity.

METHODS OF OPERATION

Attempted Acquisition of Technology

Via direct contact or through the use of front companies or intermediaries, these are attempts to acquire protected information in the form of controlled technologies, whether the equipment itself or diagrams, schematics, plans, spec sheets, or the like.

Exploitation of Cyber Operations

Attempts by foreign intelligence entities or other adversarial attempts to conduct actions to place at risk the confidentiality, integrity, or availability of targeted networks, applications, credentials or data to gain access to, manipulate or exfiltrate protected information, technology, or personnel information.

Exploitation of Insider Access

Attempts by trusted insiders to exploit their authorized placement and access within cleared industry or cause other harm to compromise protected information, technology, or persons

Exploitation of Security Protocols

Attempts by visitors or unauthorized individuals to circumvent or disregard security procedures or behaviors by cleared or otherwise authorized persons that may indicate a risk to protected information, technology or persons.

Résumé Submission

The submission of resumes by foreign persons for academic or professional placement that would facilitate access to protected information to enable technological or economic advancements by the foreign entity.

Search/Seizure

Involves temporarily accessing, taking, or permanently dispossessing someone of property or restricting freedom of movement via tampering or physical searches of persons, environs, or property.

Theft

Attempts to acquire protected information with no pretense or plausibility of legitimate acquisition.

Exploitation of Business Activities

Attempts to establish a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service provider; attempts to leverage an existing commercial relationship in order to obtain access to protected information, technology, or persons.

Exploitation of Experts

Attempts to gain access to protected information, technology, or persons via requests for, or arrangement of, peer or scientific board review of academic papers or presentations; requests to consult with faculty members or subject matter experts; or attempts to invite or otherwise entice subject matter experts to travel abroad or consult for foreign entities.

Exploitation of Relationships

Attempts to leverage existing personal or authorized relationships to gain access to protected information.

Exploitation of Supply Chain

Activities of foreign intelligence entities or other adversarial attempts aimed at compromising the supply chain, which may include the introduction of counterfeit or malicious products or materials into the supply chain to gain unauthorized access to protected data, to alter data, to disrupt operations, or to interrupt communication.

RFI/Solicitation

Attempts to collect protected information by directly or indirectly asking, petitioning, requesting, or eliciting protected information, technology, or persons.

Surveillance

Systematic observation of equipment, facilities, sites, or personnel associated with classified contracts via visual, aural, electronic, photographic, or other means to identify vulnerabilities or collect information.

Created by the Defense Counterintelligence and Security Agency. Contact us at dss.quantico.dss-ci.mbx.production@mail.mil

Collection Methods Used by Foreign Intelligence Services Cont.

DCSA COUNTERINTELLIGENCE
METHODS OF OPERATION & METHODS OF CONTACT MATRIX

METHOD OF OPERATION	Conference, Conventions or Trade Shows	Cyber Operations	Email Request	Foreign Visit	Mail	Personal Contact	Phishing Operations	Resume - Academic	Resume - Professional	Social or Professional Networking	Telephone	Web Form Submission
Attempted Acquisition of Technology	L		H	M		M				L	L	M
Exploitation of Commercial/ Business Activities	M	L	M	M		M				L	L	L
Exploitation of Cyber Operations		H	L	L		L	H			L	L	
Exploitation of Experts	L		M	L	L	L				M	L	
Exploitation of Insider Access		L	L	L	L	H				L	M	
Exploitation of Relationships	L		M	M	L	M			L	M	M	
Exploitation of Security Protocols	M	L	M	M	L	M	L			L	L	
Exploitation of Supply Chain	L		M	L						L		
Resume Submission				L		M	L	M	M			L
RFI/Solicitation	H	L	M	M		M	L	L	L	M	L	L
Search/Seizure						M						
Surveillance	M	L		L		M					L	
Theft	M		L			M						

VERSION: 18.2 – 4JUN18

THREAT/CAPABILITY H High M Medium L Low Unreported

CI Reporting Requirements

The following must be reported:

- All foreign travel and foreign contacts must be reported to an SAIC FSO/ PSO and to the customer
  - For those briefed with multiple customers you have dual reporting responsibilities
- Contact with anyone or information that suggest SAIC personnel may be the target of intelligence collection
- Contact with a known or suspected Intelligence Officer (IO)

CI Reporting Requirements cont.

- Requests by anyone for unauthorized access to SAIC sensitive information or customer information
- Actual or attempted unauthorized access to SAIC or customer IT systems

If the question even enters your mind as to whether or not you should report something the answer to that question is "YES!!!" Better to report, investigate and discover it's innocuous than not report and suffer a potential loss of personnel, information or resources.

Operations Security (OPSEC)

OPSEC is an analytic process used to deny an adversary information, generally unclassified, concerning friendly intentions and capabilities by identifying, controlling and protecting indicators associated with planning processes or operations. OPSEC is simply denying an adversary information that could harm you or benefit them.

The OPSEC process consists of five steps designed to assist in identifying information requiring protection, determining the methods that may be employed to compromise that information and establishing effective countermeasures to protect it.

OPSEC Countermeasures

Any piece of information that can be exploited to gain further information or be combined with other indicators to build a more complete profile of your operation is an OPSEC indicator.

- Keep a low profile
  - Don't "advertise" your presence or your work on social media sites
  - Don't wear contractor/customer badges in public
- Observe
  - Be aware of surroundings (environment/threats)
  - Recognize when something is wrong
  - Report suspicious activity
- Apply OPSEC – deny adversaries any information
- Identify, control and protect unclassified information related to sensitive activities to reduce vulnerabilities to our information

You are the frontline of defense against these threats. Stay alert to the threat and report any suspicious activity.

The contract you support may include OPSEC requirements. These requirements can vary from contract to contract. If you have any questions regarding your requirements, contact your SAIC FSO/PSO.

Insider Threat Overarching Guidance

An Insider Threat is: "The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits: acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace."

Drivers

Malice

Current or former employees that are triggered by a specific work–related or non–work–related incident such as a poor performance review and large amounts of debt. Insiders typically develop a plan in advance of the act that someone within the organization may detect.

- Examples: information and asset exploitation such as espionage, fraud, corruption and IT system exploitation

Insider Threat Overarching Guidance cont.

Complacency

Over time, employees may become more lax about security policies. Violators often assume that their specific behavior does not have a noticeable impact or that no one is monitoring their behavior.

- Examples: removal of proprietary or classified information or material from secure areas; forwarding information to home email addresses to work on a task after hours; inappropriately placing information in an open and unsecure area

Ignorance

Employee ignorance is a challenge to organizations attempting to manage and maintain a secure organization. Lack of understanding of security protocols and the potential impact if not followed further exacerbates the impact of unknowing exposure of critical information.

- Examples: disclosure or dissemination of information determined to be proprietary or classified to persons without clearance or purpose to have the information; irresponsible handling of classified or proprietary information; irresponsible use of information systems

Motivation

There are complex reasons why an employee would deliberately seek to cause harm. An insider will usually be motivated by one or a combination of reasons. A useful acronym to understand the motivations underlying the willing behavior is "crime".

Coercion
Being forced or intimidated

Revenge
For a real or perceived wrong

Ideology
Radicalization or advancement of an ideological or religious objective

Money
For illicit financial gain

Exhilaration
For the thrill of doing something wrong

The Critical Path to an Insider Threat

There are several factors that lead up to an individual becoming an insider threat. Many times the signs go unnoticed or are ignored. The path to an insider threat has several stages of indicators.

Not everyone who displays these is an insider threat.

Behavioral Indicators*

- Seeks or obtains access to information not related to duties
- Remotely accesses SAIC Network while on vacation, sick leave or at odd times
- Disregards company policies regarding information systems
- Overwhelmed by life crises or career disappointments
- Appearing intoxicated at work
- Pattern of disregard for rules
- Pattern of deception or lying to peers or managers
- Attempts to circumvent security controls or does not report security issues
- Short trips to foreign countries for unexplained reasons

Behavioral Indicators cont.*

There are also signs a potential insider might exhibit when under significant pressure including but not limited to:

- Unnecessarily copies materials, especially classified or proprietary
- Works odd hours without authorization, notable enthusiasm for overtime work, weekend work or an unusual schedule
- Unexplained absences on Mondays and Fridays
- Engages in suspicious contact with competitors
- Unexplained affluence; buys things they cannot afford on their income

Insider threat indicators which should be immediately reported:

- Attempts to expand access to information or IT systems without valid Need–to–Know
- History of security infractions
- Indifference towards policies
- Signs of discontent with employer
- Signs of adverse information not previously reported
- Sudden unexplained financial affluence
- Work hours inconsistent with job assignment
- Signs of conflicting loyalties toward foreign nations or industry competitors

***It should be noted that this list is only SOME of the indicators. It is important to note that many employees with motivation and malicious intent never commit an act of betrayal. If any behavior is displayed by an employee raises questions, it should be reported to your FSO/PSO and the Security Intelligence Program (SIP) immediately by emailing us: securityintelligenceprogram@saic.com.**

Anonymous reporting is available via the SAIC Ethics Hotline (800) 760-4332 or online at https://secure.ethicspoint.com/domain/en/default_reporter.asp.

Commitment to Protection of Civil Rights and Liberties

SAIC has an obligation to protect intellectual property, customer data and most importantly its employees. Any information reported to be insider threat related (real or perceived) shall be treated and protected as "SAIC Privileged and Confidential" information.

Information resulting in an investigation internally or externally shall only be shared with those who have a strict Need–to–Know. By successfully logging on to SAIC's network, the user agrees to abide by SAIC's information technology use policy and that there is no expectation of privacy while on the SAIC network.

Case Study One

CDSE Center for Development of Security Excellence

COUNTERINTELLIGENCE CASE STUDY

Counterintelligence Awareness Case Study: Kevin Patrick Mallory

What Happened?

Kevin Patrick Mallory

- Kevin Patrick Mallory was a self-employed consultant with GlobalEx LLC who spoke fluent Mandarin Chinese. He had previously held numerous positions with various U.S. government agencies and several defense contractors through which he was granted a Top Secret security clearance.
- Mallory's security clearance was terminated in October 2012 when he left government service.
- In March and April 2017, Mallory travelled to Shanghai to meet Michael Yang, who claimed to represent a People's Republic of China think tank, but—as Mallory correctly determined—Yang was actually an agent of the People's Republic of China Intelligence Service. Yang gave Mallory a smartphone so they could covertly communicate.

- Later, Mallory agreed to allow FBI agents to review a smartphone that contained a message from him to Yang that revealed Mallory had planned to travel to Shanghai with classified documents. The smartphone also held a handwritten index that described eight different documents later determined to be classified.
- FBI analysts determined Mallory had completed all of the steps necessary to securely transmit four documents using the smartphone.
- A federal jury convicted Mallory of espionage charges related to his transmission of classified documents to an agent of the People's Republic of China.

Method of Operation

- Elicitation and recruitment/targeting of U.S. travelers overseas. Foreign intelligence agents targeted Mallory due to his prior security clearance.

Impact

- One of the documents provided to the Chinese operative contained unique identifiers for human sources who had helped the United States government.
- A key objective for numerous foreign intelligence services and other entities is infiltrating the U.S. national decision-making apparatus and Intelligence Community and targeting national security information and proprietary technology from U.S. companies and research institutions.
- Counterintelligence intervention led to the disruption of these activities and prevented the loss or compromise of additional national security information.

Learn More about Counterintelligence

This case study examined a real-life counterintelligence case. Your awareness is key to protecting our national security from threats like this one. Visit the Center for Development of Security Excellence's website, https://www.cdse.edu, for additional case studies, information, materials, and training. Raise your counterintelligence awareness by visiting https://www.cdse.edu/catalog/counterintelligence.html.

Case Study Two

Insider Threat Awareness Case Study: Reynaldo Regis

What Happened?

- Reynaldo Regis worked as a cleared CIA contractor employee between August 2006 and November 2016.
- Part of his job was to research people in classified databases.
- Regis copied classified information into personal notebooks and conducted unauthorized searches of classified databases.
- Investigators were unable to determine a motive for Regis' actions. However, 60 notebooks containing classified information were found during a search of his home.
- On May 11, 2018, Regis pled guilty to unauthorized removal and retention of classified materials and making falsified statements to federal law enforcement officers.
- On November 2, 2018, Regis was sentenced to three months in prison with three years of supervised release, and the requirement to notify the CIA of any travel outside the country.

Potential Risk Indicators

- Mishandling of classified information
- Conducting unauthorized searches
- Lying to federal law enforcement
- Suspicious behavior

Impact

- The classified information found in the notebooks included data relating to highly sensitive intelligence reports, disclosure of which could cause serious damage to national security. Though Regis' motiviations are unknown, his disregard for security protocol placed this information at risk.

Learn More about Insider Threat

This case study examined a real-life Insider Threat case. Your awareness is key to protecting our national security from threats like this one. Visit the Center for Development of Security Excellence's website, https://www.cdse.edu, for additional case studies, information, materials, and training. Raise your Insider Threat awareness by visiting https://www.cdse.edu/catalog/insider-threat.html.

Export Control

The U.S. Government controls the export and release of certain products, services, and technical data to a foreign person or foreign entity. These regulations are complex. If you are supporting United States Government Operations overseas or engaged directly with foreign nationals either abroad or in the United States, you may require approval from SAIC's International Trade Compliance Department in ADVANCE of any of those discussions or travel!

ALWAYS seek advance guidance from the International Trade Compliance department before discussing, marketing, selling, emailing, or otherwise transferring information to a foreign person.

Export Compliance

An export includes sending or taking an item out of the U.S., release of technical data to a foreign person, and any service performed for a foreign person in the U.S. or abroad. This also includes training or presenting.

Foreign persons include embassies in the U.S., foreign companies, and foreign nationals in the U.S. It is important to note that this includes foreign nationals employed by U.S. companies, including any foreign national colleagues at SAIC.

Keep in mind that technical data transfers also include oral presentations and demonstrations, emails, texts, or other electronic transmissions, telephone conversations and marketing presentations, and brochures.

International Traffic in Arms Regulations (ITAR)

International Traffic in Arms Regulations (ITAR) are regulated through the State Department's Directorate of Defense Trade Controls (DDTC).

ITAR controls highly sensitive defense articles, services and technical data. If the item is ITAR controlled (on the U.S. Munitions List), it will require an export authorization.

Export Administration Regulations (EAR)

The Export Administration Regulations (EAR) are regulated through the Commerce Department's Bureau of Industry and Security.

The EAR controls dual-use articles and technical data and is less restrictive than ITAR. You may or may not require an export authorization for exporting an EAR or commercial item. It will depend on the final destination country, classification of the item, and the end-user. Always seek SAIC's International Trade Compliance department before shipping, emailing, or providing any information to a foreign end-user-even if it relates to what you would consider a commercial item..

The main difference between ITAR and EAR is ITAR is more restrictive than EAR and ITAR controlled items will always require authorization while EAR controlled items may not depending on the situation.

Export Administration Regulations (EAR) cont.

You must ALWAYS coordinate in advance with the International Trade Compliance Department to get a product classification, so your shipment or communication is treated within compliance of the law.

Licenses and Technical Assistance Agreements (TAA)

Projects that provide services or technical data to foreign persons and/or entities may need to apply for a license or Technical Assistance Agreement (TAA).

- Don't export commodities, perform a defense service or provide technical data without an export license, agreement or exemption and proper documentation
- Keep in mind that a license or TAA can take three to six months to process

For additional information on International Trade Compliance and International Business, contact International Trade Compliance. Specific points of contact are available on ISSAIC.

International Trade Compliance Department

What International Trade Compliance (ITC) can do for you!

International solutions that keep you, SAIC and your customers safe and productive.

Compliance with the law

Approval and authorization to conduct and support international activity is required.

International Travel

The newly revised International Travel Review System (ITRS) captures information that streamlines your needs for International Trade Compliance, Cybersecurity, High Risk travel, Insurance needs, Foreign Travel filing requirements for those with a Security Clearance.

Required Recordkeeping

Did you know that all international trade compliance must be documented and maintained for 5 years after that expiration of your activity? Use of exemptions, licenses, TAA's or other authorizations must be documented fully to comply with the law. Coordinate with ITC in advance!

International Trade Compliance Reminders

All SAIC employees are responsible for, and have a role in preventing violations – U.S. Trade controls affect all functions and roles:

- **Human Resources:** Hiring foreign nationals
- **Procurement:** Engaging sales representatives, Procuring foreign items and services
- **Business Development:** Marketing foreign entities/persons
- **Line Organizations:** International travel, Performing FMS contracts, Contracts with or involving foreign persons, Discussions/exchanges with foreign persons or entities
- **Security:** Compliance with the NISPOM and clearance requirements; Foreign visitors
- **Treasury:** Insurance requirements for contracts involving overseas performance
- **Cybersecurity:** Laptop and other device restrictions

Whenever there is a foreign entity, i.e., individual, company, or government involved. You must engage SAIC ITC. This includes foreign person visits and international travel – know before you go!

International Authorizations are complex, please allow plenty of lead time for ITC to manage any potential, licensing or authorizations through Department of State and/or Department of Commerce.

Engage SAIC ITC early and often. ITC strives to be your partner on all things International and can be your headlights or the emergency brake to your program and/or international activity.

Product of the Office of Security

122215