



SAIC Security
Protect the Mission. Secure the Future.

ANNUAL SECURITY REINDOCTRINATION (ASR)

DESK REFERENCE

Please direct questions to your local Facility Security Officer (FSO) or Program Security Officer (PSO).

January 2025

Section 1: Safeguarding Sensitive Information and Data	Pages 4 - 12
• CUI.....	4 - 8
• Other Protected Data.....	9 - 10
○ PII/PHI	
○ Proprietary and Material Information	
• Sharing Information Safely	10 - 11
• Proper Data Storage.....	11 - 12
Section 2: Cybersecurity Awareness & Protections	13 - 17
• Overview	13
• Cybercrimes Concerns.....	13 - 15
○ Phishing	
○ Ransomware	
○ Social Media	
• Insider Threat	15 - 17
○ CRIME Acronym	
○ Behavioral Indicators	
○ Doing Your Part	
Section 3: Securing SAIC Assets.....	17 - 20
• Protected Email Use.....	18
• Protected Hardware Use	18 - 20
○ Laptop Security	
○ Mobile Devices	
○ Removable Storage Devices	
○ Printer Use at SAIC	
Section 4: International Trade Compliance & Crisis Management	21 – 26
• Export Compliance	21 - 22
○ Export Controlled Info	
○ Foreign Persons/US Persons	
○ ITAR	
○ EAR	
• Export Controlled Shipments	22 - 23
○ International Shipments	
○ Export Authorization	
○ Export Licensing	
• International Business Conduct	24 - 25
○ Foreign Corrupt Practices Act	
○ SAIC FCPA Policy SI-POLI-07	
• International Travel	25
○ ITRS	
○ ITC on SAIC	
• Crisis Management and Business Continuity.....	25 - 26

Section 5: Cleared Security Awareness 27- 44

- Understanding Security Clearances 27 – 29
 - Clearance Types
 - CE/CV
 - Eligibility
 - NDA
- 13 Adjudicative Guidelines 29 – 32
- Reporting for Cleared Personnel 32 – 34
- Safeguarding Information 34 – 36
 - Handling Classified
 - Data Spillage
 - Security Violations
- Classification Management..... 36 – 40
 - Classification Levels
 - Classification Marking
 - Working Papers
 - Prohibitions, Limitations and Sanctions
 - Safeguarding Classified Information
- Physical Security 40 – 44
 - Badges
 - Visitor Access
 - Controlled Spaces
 - Prohibited Items
 - Classified Meetings

Section 6: Counterintelligence..... 45 – 51

- Recognizing Threats..... 45 – 50
 - External Threats
 - Collection Methods
 - OPSEC Process
 - OPSEC Countermeasures
- Counterintelligence Reporting Requirements..... 50 – 51
 - Reporting CI Threats
 - Reporting Personal Changes
 - Reporting Check

SECTION 1: SAFEGUARDING SENSITIVE INFORMATION AND DATA

Information Security

In your role at SAIC you may work with sensitive information, either owned by SAIC or our customers. No matter where or how we work, we must always remember that protecting sensitive information is paramount.

Sensitive Data Precautions

Sensitive Information Awareness

Information and data are the lifeblood of SAIC and our customer's business. We must be guardians of all information and data. It is critical you are aware of how to identify, store, and properly disseminate sensitive information.

Controlled Unclassified Information (CUI)

CUI is sensitive, unclassified information that requires protection under laws, regulations or Government-wide policies. All CUI is government-created or government-owned, requires specific security measures, and represents many different categories. During your work at SAIC you may work with or come in contact with CUI.

Working with CUI

There are two categories of CUI – Basic and Specified



CUI Basic requires protection but does NOT set out specific handling or dissemination controls.



CUI Specified sets out specific handling or dissemination controls determined by specific agencies or organizations.

Let's work through the lifecycle of CUI:



Identify CUI

The identification of CUI is critical for determining what sensitive information needs to be protected. It is important to understand what information is designated as CUI and what information is not CUI. CUI is a **designation** and should not be confused with Classified information.

CUI Is:

- Government-created or -owned.
- Created for the Government by contractors.
- Requires specific security measures.
- Represents many different categories.

CUI Is Not:

- Classified information.
- Corporate Intellectual property (unless created for included in contract requirements)
- Publicly available information

CUI markings can only be designated by the Government and may not be used by anyone else for any other purpose.

CUI markings **cannot** be used to:

- Conceal violations of the law, inefficiency, or administrative errors
- Prevent Embarrassment to a person, organization, or agency.
- Prevent open competition.
- Control unprotected information.
- Circumvent the Freedom of Information Act (FOIA) requests.

CUI Designation

The Information Owner (IO) of a document or material is responsible for determining whether the information falls into a CUI category using one of two registries. If the material is CUI, appropriate markings and dissemination controls are applied.

Information owners include:


- DoD civilian and military personnel
- Agencies
- Contractors (like SAIC) providing support to the DoD via a contract requirement.

Available CUI Registries

[ISOO Registry](#) and [DoD Registry](#)


1 [ISOO Registry](#)

The National CUI Registry contains Indexes and categories for the entire Executive Branch and should be consulted for non-DOD contracts.



2 [DoD Registry](#)

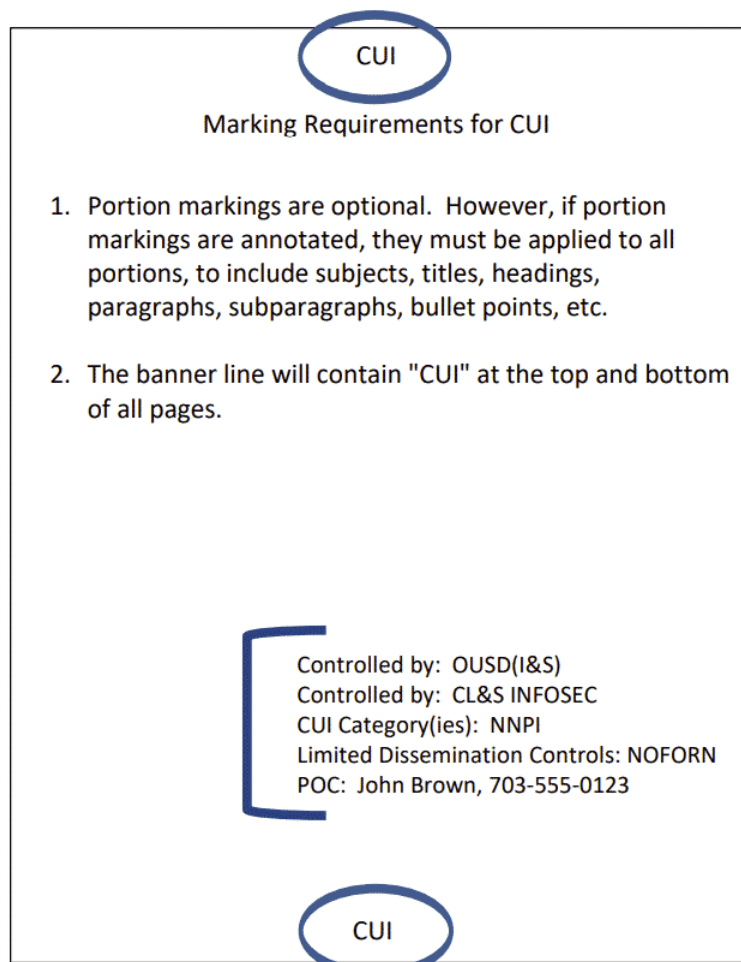
The DOD CUI Registry aligns each Index and Category to DOD issuances.



Mark/Label CUI

All physical and digital media must be **marked** or **labeled** by the "IO" to alert individuals to the presence of CUI. Markings must include:

- Header/top/banner of the document must have CUI or CONTROLLED in bold letters (bottom is optional)
- Designation Indicator including:
 - Who owns the information?
 - Who controls the information?
 - Type of CUI contained in the document (CTI, OPSEC, etc.)
 - Distribution/Limited Dissemination Control (LDC) information
 - Main contact or POC



Storing CUI

Per the DoDI 8500.01, Systems processing CUI will be categorized at no less than the moderate confidentiality impact level in accordance with Part 2002 of Title 32, Code of Federal Regulations (Reference (z)).

Dissemination of CUI

Distribution Statements define who is eligible to receive CUI. The "IO" must apply distribution markers to CUI export controlled technical information, other scientific, technical and engineering information, and controlled technical information.

Limited Dissemination Control (LDC) Statements transfer power to the agencies themselves to place distribution limits on CUI. Be aware of and abide by LDC statements when working with CUI.

Destruction of CUI

CUI policy requires that agencies and organizations destroy CUI in a manner that makes it unreadable, indecipherable, and irrecoverable.

Decontrol of CUI

Employees and contractors should contact the Information Owner to discuss decontrolling (downgrading) the CUI material when the need arises. Impetus to request decontrol may include:

- Request to release the CUI material to the public
- End of contract
- Contract renewal

BE AWARE: Sending CUI to personal email accounts is strictly prohibited and will result in disciplinary action.

Store

System Storage

The NIST SP 800-171 governs and protects CUI on non-Federal Information Systems

Physical Storage

During Working Hours

- Personnel must take care not to expose CUI to unauthorized users or others who do not have a lawful government purpose to see the information.
- CUI cover sheets (not required) may be placed on top of documents to conceal the contents from casual viewing.
- Always control or protect CUI with at least one physical barrier and take reasonable care to ensure the information is protected from unauthorized access and observation.

After Working Hours

- Store in unlocked containers, desks, or cabinets only if facility provides continuous monitoring. If not, CUI must be in a locked desk, file, cabinet, locked room or where security measures are in place to prevent or detect unauthorized access.

Other Protected Data

Personally Identifiable Information (PII)

PII is information that, when used alone or with other relevant data, can directly or indirectly identify an individual. To include:

- Social Security Number
- Data or place of birth
- Mother's maiden name
- Driver's license number
- Other private information associated with an individual that can be used for identification purposes.

Personal Health Information (PHI)

PHI is information about health status, provision of health care, or payment for health care created or collected by a Covered Entity and can be linked to a specific individual. To include:

- Medical history
- Test and lab results
- Mental health conditions
- Insurance information
- Other data gathered by healthcare professionals to identify an individual and determine appropriate care.

PII/PHI Protection

SAIC policy SI-POL1-05 Data Privacy and Protection establishes the requirements and responsibilities of SAIC employees when they use PII or PHI data. This includes:

- Creating a Privacy Plan for each contract, statement of work, task order or functional organization that uses PII/PHI.
- Training for employees who handle this privacy data.
- Safeguarding the data and its dissemination.
- Immediately **reporting** all actual or suspected data breaches or data loss to all of the following: immediate supervisor, ITO Cybersecurity Team, and the appropriate security point of contact.
- Do not share PII/PHI with those not authorized to use or view the data

Proprietary and Material Information

Proprietary information is information owned or possessed by SAIC and **not** authorized for public release. Material information, although proprietary, is information likely to be considered important to investors and their decision to purchase or sell SAIC securities. This information is highly valuable to our company and must be protected. Examples include:

PROPRIETARY INFORMATION	MATERIAL INFORMATION
<ul style="list-style-type: none"> • Financial data • Technical data • Trade secrets • Proposal and contract data • Business development materials • Business processes • Strategy information • Pricing information • Intellectual property • Other business information of value to the company such as reports, presentations and internal correspondence containing any of the above 	<ul style="list-style-type: none"> • Financial results and projections • Changes in senior management, company's accountants or accounting policies • Company strategic plans • News of a potential merger/acquisition or sale of company assets, securities or subsidiaries • Significant labor disputes or negotiations • Gain/loss of a major contract, order, customer, supplier or financing source • Actual/threatened major litigation or the resolution of such litigation • Government investigations, reviews or audits • Major product/service announcements • Impending bankruptcy or the existence of severe liquidity problems • Stock splits, public or private securities/debt offerings, or changes in company dividend policies or amounts • Capital investment plans and changes in such plans • Purchases or redemptions by the company of its own securities • Any other major problems or successes of the business

Sharing Information Safely

Data and File Sharing Protections

Sensitive data must be protected when at rest and when shared.

Encryption

Encryption is the best way to protect sensitive information in transit, sent by email, or at rest. SAIC approves the following **methods of encryption**:

- PKI and DoD External Certificate Authority (ECA)
- Card Tokens for encrypting and digitally signing email (PIV/CAC)
- Secure File Transfer Protocol (SFTP) utility

Certain types of data shared via SAIC email require additional protection based on the category of data and the intended recipients of the email. When sending email containing sensitive information, be aware of the following encryption requirements:

Email to SAIC.com address:

- PHI/PII
- Information related to cyber and security incidents.
- Information related to investigations.
- Information related to matters marked “attorney client privileged”

Email to (opens in a new tab)external address:

- CUI
- PII

- PHI
- SAIC proprietary information
- SAIC intellectual Property
- Sensitive Financial information

Collaboration Tools

SAIC provides tools such as ZoomGov and Microsoft Teams to conduct business and collaborate. These tools allow you to securely hold meetings, send files, and communicate with instant messaging with each other and your customer.

Things to remember when using collaboration tools like Zoom or Teams:

- Instant messages must **not** contain any material that may reasonably be considered offensive, disruptive, defamatory, or disparaging.
- Recording of Zoom or Teams calls is **disabled** unless there is a compelling business reason.
- You have **NO** expectation of privacy when using SAIC collaboration tools.

ZoomGov IL4

If you are required to hold meetings where CUI may be discussed or shared with **external** customers, request a ZoomGov IL4 account via ES3 **ahead** of time.

You may only use approved methods for sharing files and information such as Teams, OneDrive, SharePoint and SFTP.

No matter how or where we work, protecting sensitive information is critical.

Proper Data Storage

Data Storage Protection

Cloud Storage Usage

Protecting our most sensitive data means SAIC and customer data must not be stored using public cloud-based storage services, unless such storage has been approved by Cybersecurity.

Placing SAIC or customer data in a public cloud environment may subject SAIC to severe penalties, sanctions, or other legal actions.

Cloud based storage or data exchanges must be:

- SAIC approved

- FedRAMP moderate
- Encrypted, *in transit and at rest*

Personal cloud storage services such as iCloud, Dropbox and Google drive are strictly **prohibited**.

Physical Data Protection and Destruction Considerations

Sensitive data requires protection including proper handling, storage and destruction.

Sensitive Data Destruction

- Place discarded sensitive data in properly locked and labeled destruction bins within SAIC or customer facilities.
- Home shredders are not approved for destruction of sensitive data.
- Do not stack sensitive data on full bins. Store in a locked cabinet until a bin is available.
- Understand the requirements of your customer/contract for data storage and destruction.

Everyone must be diligent and practice good data storage and protection hygiene.

SECTION 2: CYBERSECURITY AWARENESS & PROTECTIONS

Cybersecurity is a shared responsibility. Every employee has a responsibility to protect company and customer data from loss, theft, and misuse.

Cybersecurity is a top priority at SAIC.

We are constantly challenged by new attacks, new requirements, and new technology. While the Cybersecurity team works diligently to support SAIC with a 24/7/365 defense and threat response, it is vital for all employees to understand and take **responsibility** for their role in protecting the company.

Together, we can ensure SAIC's impeccable reputation is **protected**, and our customers continue to entrust us with their data.

Cybercrimes Concerns

Be Aware of Cybercrime

SAIC employees are often targets of cybercrime due to our work with the government and access to information related to national security. Malicious hackers and criminals carry out cybercrime to exploit others and steal valuable information and data.

Phishing

Phishing is a social engineering attack that targets companies like SAIC. It is one of the many threats we face every day as SAIC employees. Attacks are carried out through fake emails, text messages, and phone calls.

Verify the Sender

Verify the sender is a contact known to you and is a valid email address `it@verifypass.pw` is not a valid SAIC email address.

Proceed With Caution When You See an External Sender

SAIC has configured your inbox to label all external emails with a red warning. Treat the warning as your cue to read external emails very carefully before acting.

Don't Trust all Email Addressed Directly to You

Beware - you may receive phishing emails that are directly addressed to you. An attacker may have your name from social media like LinkedIn or a data breach.

Don't Skim an Email Just Because it Looks Ordinary

Attackers try to take advantage of common, real-world scenarios and activities to lend to their email's credibility. Common uses are password changes, invoices, shipment notifications, and offers for marketing lists.

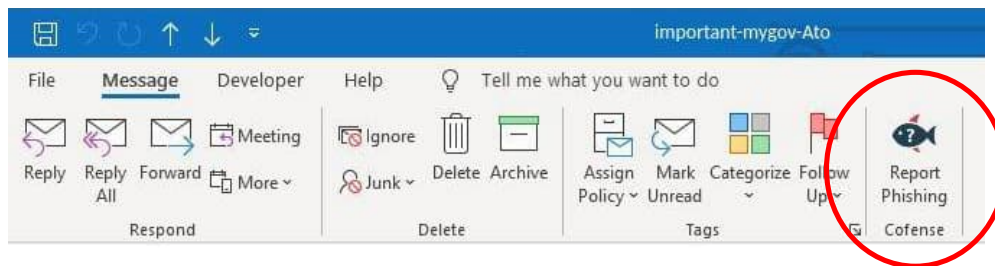
Think Twice Before You Click

The Check Password link looks pretty convenient - but it is a trick to redirect you to the attacker's own site so they can collect your credentials. "Hover for cover" and carefully hover your mouse (without clicking!) over buttons and links to see the real address where they want to take you. Additionally, consider if this process seems in line with our company processes and policies.

Sense of Urgency

Phishing emails often contain a sense of urgency or negative consequence if you do not act soon. Question the action - does it seem reasonable?

How to report Suspicious Email



From the email message, click on the Report Phishing icon on the message ribbon or forward the email to fraudalert@saic.com.

Ransomware

Ransomware is a lucrative type of malware that encrypts the targeted system(s) to withhold access to those systems from the victim until a ransom payment is received. It is often introduced into a network via email or other types of social engineering.

BE AWARE: If you receive a threatening message demanding payment, disconnect you system from the network and call **833-YO-CYBER (833-962-9237)** right away.

Social Media



Social networking sites are a great way to connect and share information. However, the amount of visitors these sites attract makes them extremely **vulnerable** to cyber criminals. **Review** your privacy settings often and be **cautious** of what you reveal in online forums to include customer or company information.

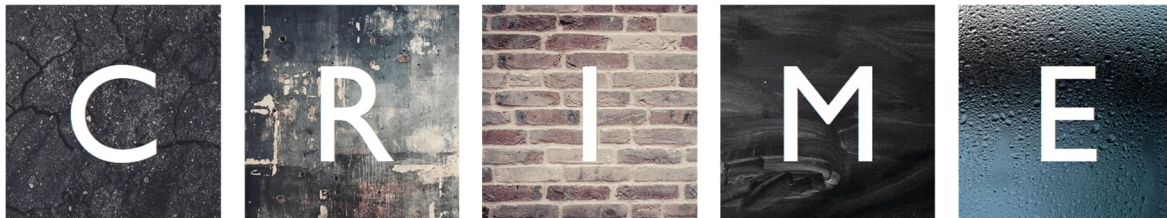
Don't Make Yourself a Target!

Insider Threat

Recognizing Insider Threats

Insider threats come from persons who have or have had authorized and legitimate access to a company's assets and abuse it either deliberately or accidentally.

There are complex reasons why an employee would deliberately seek to cause harm. Insiders are usually motivated by one or a combination of reasons. The useful acronym to understand motivation is "CRIME"



Coercion is defined as 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

Behavioral Indicators

Certain behavioral patterns, while not necessarily an indicator of malicious intent, may warrant careful attention and proper reporting. Here are a few things to watch out for:

Information Access

- Seeks to obtain access to information not related to their duties
- Remotely accesses company network while on vacation, sick leave, or at odd times
- Attempts to circumvent security controls or does not report security issues
- Downloads or sends large amounts of data to personal email accounts

Disregard for Rules

- Disregards company policies regarding information systems
- Pattern of disregard for rules
- Pattern of deception or lying to peers or managers

Personal Life

- Overwhelmed by life crises or career disappointments
- Appears intoxicated or under the influence at work
- Frequent, short trips to foreign countries
- Fixation on ideological web sites or social media

Vigilance is everyone's responsibility

Vigilance in Your Surroundings

- **Suspicious Activities or Persons** – people or events in or around facilities that appear unusual
- **Facility Safety Problems** – unsafe building operations, malfunctions, or hazards
- **Workplace Disruption** – employees exhibiting behavior that may harm themselves or those around them

Suspicious Behaviors

- **Counterintelligence or Espionage** – suspicious contacts or attempts to solicit sensitive information from or about SAIC or its customers
- **Misuse of Resources** – IT systems, inappropriate material, or use for personal business
- **Security Violations** – violations of protocol related to classified programs

Responsibility to Report

Every SAIC employee has a responsibility to report unusual or suspicious behaviors. You can report via the Security page on ISSAIC.

Doing Your Part

Your role in the security process has three parts:

1. Follow SAIC policy and guidance
2. Be alert and aware in your daily activities. Use good judgement when working with SAIC information and systems.
3. Report anything suspicious or out of the ordinary.

SECTION 3: SECURING SAIC ASSETS

Protected Email Use at SAIC

A cornerstone of communication and information sharing at SAIC is our corporate email. You are required to use and maintain an SAIC email address for official SAIC correspondence. You may also be assigned a customer-specific email account for program-related correspondence.

NOTE: If you are assigned to a customer location, you are encouraged to check your SAIC email at least weekly in order to receive important corporate updates and information.

SAIC correspondence is:

- SAIC corporate news and updates
- Messaging from SAIC leadership
- Non-program specific correspondence

Forwarding SAIC or customer information/data to personal email accounts is strictly prohibited.

SAIC Email Restrictions

In order to protect SAIC information and data, it is critical you use your SAIC email account responsibly. The following practices are strictly **prohibited**:

- Forwarding SAIC or customer information or data to a personal email account for any reason. *Documents or information pertaining to employee personal information are permissible (i.e. tax, benefits, education).*
- Using third-party or external email service providers for SAIC business-related email
- Accessing Web-based email accounts, such as Gmail and Hotmail
- Downloading email attachments from Outlook Web Access (OWA) to personal devices

Keep in mind – you have no expectation of privacy as it relates to your SAIC email account and misuse can lead to disciplinary action.

Protected Hardware Use at SAIC

The Acceptable Use Policy sets the guidelines for using and protecting SAIC assets properly. SAIC assets should **not** be used for purposes outside of SAIC or customer business.

Let's look at common assets – SAIC and personally owned – that require protection:

Laptop Security

- Don't make **unauthorized** changes to your laptop.
- Installing non-SAIC provided or authorized software is **prohibited** without prior authorization by ITO.
- Don't allow **others** to use your laptop or account.
- Be **aware** of your surroundings when sensitive data is on your screen.
- Always **lock** your laptop when stepping away.
- **Report** lost or stolen SAIC assets immediately.

You cannot take your SAIC laptop outside the U.S. without prior authorized permission from SAIC Security and the International Trade Office.

Mobile Devices:

SAIC's Personal Device Program (PDP) allows use of your mobile devices to conduct SAIC business. (*Instruction SI-ITS-04*)

- You **must** register your device prior to downloading SAIC or customer data to your device.
- Do not share **sensitive** SAIC or customer data via **text** or unencrypted email on your personal device.
- Do not conduct SAIC business on personal devices outside of SAIC-approved mobile apps.
- Maintain **positive** control of your device at all times.

Do not let unauthorized personnel view customer or SAIC data on the device.

Your device must be enrolled in PDP before accessing SAIC email while in a foreign country.

Lost or stolen devices enrolled in PDP must be reported to Cybersecurity and Office of Security immediately.

Removable Storage Devices:

Removable media storage devices are prohibited for use at SAIC unless an approved exception has been granted for specific business operations.

- Do not **store** sensitive customer or SAIC data, data categorized as CUI, PII, or PHI on unapproved and unencrypted devices.
- Do not **plug in** any removable device into an SAIC computer unless the device has an identified owner and has been authorized for use.

Devices such as thumb/USB drives and external hard drives can bring malware into a computer and its networks.

Printer Use at SAIC

Printers are available for use at SAIC and customer locations. Use of these printers is allowed for business printing only. If working remote, you **must** have an SAIC issued printer in order to print SAIC or customer data. Printers **not** managed by SAIC are at risk for data theft or compromise.

Prohibited Printer Use

- Printing SAIC sensitive or proprietary information on home printers, or other printing devices **not** issued by or managed by SAIC
- Printing information that **contains CUI** while at home or working remotely, such as when on travel
- Leaving sensitive information, including CUI, **unattended** on an authorized printer

Printing Options/Alternatives

- Digitally sign documents with PDF-Exchange Pro
- For expense reporting, take a picture of your receipts with your mobile device and upload to your Expense Report
- Travel to an SAIC location to print documents that require physical printing
- If you have a compelling business requirement to print, submit a request via ES3

Check out SAIC Acceptable Use Policy on ISAIC for more information. Violations of the Acceptable Use Policy carry significant consequences up to and including termination.

SECTION 4: INTERNATIONAL TRADE

SAIC is committed to conducting international business in compliance with U.S. laws and regulations.

International Trade Compliance

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, also known as ITC, in **advance** of the following:

- Discussions where a foreign national will be in attendance
- Exporting technical data, hardware or software
- International travel

If you are unsure if your program supports overseas operations or engages with foreign nationals, check with your supervisor.

Export Compliance

Did You Know?

An export doesn't just include items you generally think of like crops, oil, or even car parts. Potential SAIC exports include the following:

- Sending or taking an item out of the U.S.
- Release of technical data to a foreign person
- Any service performed for a foreign person in the U.S. or abroad

Export Controlled Information

Any information being shared with a non-US Person, otherwise known as a Foreign person, must be reviewed and approved by SAIC's International Trade Compliance Department via SAIC's Export Authorization Request System (EARS) **prior** to any information sharing takes place.

Understanding the Players

Foreign Persons

Foreign person includes embassies in the U.S., foreign companies and foreign nationals in the U.S. This also includes foreign nationals employed by U.S. companies, including SAIC, and U.S. persons employed by foreign companies.

U.S. Persons

A U.S. Person is someone who is a U.S. Citizen, U.S. incorporated entity, an individual with U.S. permanent residence (“Green Card” holder), or a “protected person” under Section 8 of the U.S. Code



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 items can be found on the U.S. Munitions List and will require an export authorization.

Export Administration Regulations (EAR)

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

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 controlled item (on the Commerce Control List). It will depend on the final destination country, classification of the item and the end user.

You must ALWAYS coordinate in advance with ITC to get the correct export classifications to ensure your shipment or communication is treated within compliance of the law.

Strict penalties such as fines and/or imprisonment can result from improperly or illegally sharing or exporting items. This is not just for SAIC, but you, as an individual, are also subject to U.S. Trade Regulations and can be fined or imprisoned for violations.

Export Compliance is complicated. Reach out to ITC early for assistance!

Export Controlled Shipments

International Shipments

All international shipments of hardware or physical goods must be screened by ITC in advance. This ensures compliance with the ITAR and the EAR. ITC screens shipments based on the following:

- End-user
- Destination country
- Export classification
- Schedule B number
- Value
- Other considerations

All international shipments must be **cleared** by ITC regardless of value. **Seek** guidance from ITC for more details on compliance screening and authorization prior to shipment.

All SAIC employees who ship internationally must complete the International Shipping Compliance training module available on SAIC Learning.

Export Authorization

The Export Authorization Review System (EARS) is a tool used by SAIC employees to request International Trade Compliance (ITC) approval for all exports. This enables the ITC team to track, approve, and store export requests. Any program planning to export under contract authority is required to submit a request through this system.

Possible Exports May Include:

- Shipments of hardware
- Exchange of software
- Emails and phone conversations
- Taking a laptop out of the country
- Performing services for foreign nationals
- Conversing with foreign nationals at an SAIC facility
- Working under a Foreign Military Sales (FMS) contract

Export Licensing

Projects providing exports such as services or technical data to foreign persons and/or entities may need to apply for a license or Technical Assistance Agreement (TAA) prior to export or shipment.

You must have an **approved** export license, agreement, or exemption in place for the following:

- Exporting commodities
- Performing a defense service
- Providing technical data

START EARLY! Obtaining a license or TAA can take 3-6 months to process.

International Business Conduct

The Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act (FCPA) governs the conduct of international business and carries stiff penalties.

Antibribery Precautions

Under the FCPA, it is **unlawful** for a U.S. person or company to offer, pay, or promise to pay money or anything of value to any foreign official for the purpose of obtaining or retaining business. It criminalizes bribery as a means of obtaining or retaining business overseas or seeking an **unfair advantage** in obtaining or performing such work.

Before offering a gift, hospitality or other business courtesy to a foreign official, ask yourself these questions:

1. Does the recipient foreign official have authority or influence over decisions affecting SAIC business or ability to deliver on our contract?
2. Can the gift be easily monetized, i.e., readily sold or exchanged?
3. Did the foreign official request the business courtesy or specify its expected value or kind?
4. Is there secrecy surrounding the offer?

Facilitating payments (e.g., to expedite the customs processing of goods) are prohibited. Report any facilitating payment attempts by foreign persons to ITC.

Gifts & Gratuities Considerations

- Any meal shall conform as closely as possible to U.S. government per diem rates.
- Any travel accommodation, including lodging and airfare, shall conform to travel regulations and standards applicable to U.S. government contracts.
- Any gift shall be limited to tokens of esteem such as company logo items; no items with inherent cash value or those that can be exchanged for cash.

Review SAIC FCPA policy prior to conducting any international business.

[SI-POL11-07](#)

International Travel

International travel increases risks related to export control, cybersecurity and personnel security.

Travel with Approval

International Travel Review System (ITRS)

ITC reviews all international travel requests (ITR) and provides guidance and oversight for corporate-wide compliance with U.S. export, import, and sanctions regulations. Prior to booking travel you must complete and International Travel Request.

- Visit [ITC's ISSAIC page](#) for a [link](#) to submit ITRs and access to other international travel resources.
- All SAIC personnel who hold any type of clearance must submit an ITR **prior** to travel.
- Review [SAIC policy SI-POL1-07](#), Complying With the Foreign Corrupt Practices Act (FCPA), prior to submitting an ITR.
 - The ITR must have **final approval** before booking travel through Concur.
 - Note: The ITR can take up to 5 days to review and approve travel requests.

An International Travel Request (ITR) must be submitted prior to any travel outside the United States, including U.S. territories (Guam, Puerto Rico, etc.). More information on ITRs can be found on the ITC page on ISSAIC.

Crisis Guidance and Business Continuity

The safety and security of our employees is of the utmost importance, both onshore and overseas.

Visit the Crisis Guidance site on ISSAIC to access the following:

Information on emergency preparedness, weather events and personal preparedness

- Instructions on time-charging in the event of a crisis
- Contact information for the Corporate Business Continuity Team
- Corporate Emergency Preparedness Plan
- Site-specific Emergency Procedures

Emergency Notification:

In support of our commitment to safety, it is **imperative** your personal contact and emergency contact information **is up to date on MyHR**. Be sure to update your information at least **annually**.

You can refer to the International SOS Information on the [ISSAIC International Security](#) page for employee assistance or support while overseas. To request a country intelligence report, please contact L_Crisis_Management_Team@saic.com.

Use the SAIC member number 11BYCA083835

SECTION 5: CLEARED SECURITY AWARENESS

Understanding Security Clearances

Clearance Types

Employees may be granted one of the following types of security clearance and must accept the responsibility of that privilege.

- Confidential
- Secret
- Top Secret

Interim Clearance Eligibility

Interim clearance eligibility is a restricted clearance determination granted to individuals in process for a final Confidential, Secret or Top Secret security clearance adjudication determination.

An Interim Confidential or Secret is valid for access to classified information at the level of eligibility granted but is wholly restricted from access to any level of special handling information including Restricted Data, COMSEC and NATO information until the final clearance determination is made.

An Interim Top Secret is valid for access to Top Secret information but is restricted from access to special handling information including Restricted Data, COMSEC, and NATO information at the TOP SECRET level until the final clearance determination is made. However, Interim TS permits access to restricted information at the CONFIDENTIAL and SECRET levels, provided the appropriate need-to-know is established.

Interim Confidential		Interim Secret		Interim Top Secret	
CAN ACCESS	CAN'T ACCESS	CAN ACCESS	CAN'T ACCESS	CAN ACCESS	CAN'T ACCESS
Confidential	Confidential RD	Confidential	Confidential RD	Confidential	Top Secret RD
	Confidential NATO	Secret	Confidential NATO	Secret	Top Secret NATO
	Confidential COMSEC		Confidential COMSEC	Top Secret	Top Secret COMSEC
	Secret of Any Kind		Secret RD	Confidential RD	SCI of Any Kind
	Top Secret of Any Kind		Secret NATO	Confidential NATO	
	SCI of Any Kind		Secret COMSEC	Confidential COMSEC	
			Top Secret of Any Kind	Secret RD	
			SCI of Any Kind	Secret NATO	
				Secret COMSEC	

Continuous Evaluation/Continuous Vetting

In June 2022, the Office of the Undersecretary of Defense (OSD) announced the elimination of Periodic Reinvestigations, a significant shift affecting the contractor population cleared under the National Industrial Security Program, including DoD and branch services agencies, DIA, NGA, NSA and DoS. In its place, an updated SF86 must be submitted every 5 years from the date of the last background investigation or CV enrollment, whichever is more recent, regardless of level of eligibility and access.

Similarly, though not yet formalized, most other IC agencies except USG are no longer conducting PRs as a standard. However, ALL agencies may still conduct these formal investigations on an as needed or requested basis.

To learn more about the Continuous Evaluation process, visit the following: [Office of the Director of National Intelligence](#)

SF86

You will be required to submit an SF86 (or equivalent) at the 5-year investigation date, CE/CV enrollment anniversary, or when requested by the government that sponsors your clearance.

In some instances, the government may still conduct a full reinvestigation. SAIC Security will notify you when appropriate paperwork is required. Keep in mind, clearances do not expire while in current access and enrollment in CE/CV.

Eligibility

Eligibility is a person's ability to gain access to classified information. The following must be completed to gain "eligibility" or a clearance:

- Background Investigation
- Adjudication Determination
- Polygraph Participation Consent (if required)

You must have a **Need to Know** and be **formally briefed** on a program before your clearance becomes active.

Need to Know is a prerequisite for protecting classified information. It prevents unauthorized disclosure of sensitive and classified information

Non-Disclosure Agreements (NDA)

You must sign an NDA to maintain access to a Program. An NDA is a life-binding contract between you and the U.S. Government. Under an NDA you:

- Will not reveal classified information to an unauthorized person
- Are subject to penalties for U.S. code violations
- Are required to submit information planned for public release

You **must report to SAIC Security any specific information that has an effect on your clearance status, even if it may affect your continued eligibility to access classified information. Reportable information must go to ALL agencies holding your clearance status**

Adjudicative Guidelines

13 ADJUDICATIVE GUIDELINES

All cleared personnel have a duty to report specific information to security as it occurs, even if the information affects your continued eligibility to access classified information. All reportable information must go to all agencies that you hold a clearance through.

SAIC refers to the **13 Adjudicative Guidelines** to determine what should be reported.

The Department of Defense (DoD) and Intelligence Community (IC) has set forth **13 Adjudicative Guidelines** in the DoD Directive 5220.6 and Director of National Intelligence, Security Executive Agent Directive 4 (SEAD 4) to determine initial or continued eligibility for access to classified information.

Additionally, SEAD 3 - Reporting Requirements for Personnel with Access to Classified Information or Who Holds a Sensitive Position established standardized reporting requirements across the federal government for cleared individuals. You must report these requirements to your SAIC Facility Security Officer (FSO) or Program Security officer (PSO) when they occur.

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

1) Allegiance to the United States

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

2) 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

3) 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: possession of a valid foreign passport

4) 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

5) 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

6) 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

7) Alcohol Consumption

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

8) Psychological Considerations

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

9) 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

10) 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

11) Use of Information Technology Systems

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

12) 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

13) 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**

Reporting for Cleared Personnel

A Privilege, Not a Right

Holding a security clearance is a privilege, not a right. When you accept the privilege of access to classified information, you are also accepting the responsibilities that accompany this privilege.

Adverse Information

Adverse information is any information that may unfavorably reflect 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 may not be in the interest of national security.

Reporting Responsibility

When you accept the privilege of access to classified information, you are also accepting the responsibilities that come with it; the investigative and adjudicative process and behavior that might jeopardize your clearance. Reporting is one of the responsibilities that comes with a clearance.

The following lists highlight activities that are reportable at each clearance level.

Please Note: The lists are not all inclusive. Cleared personnel should consult with their local FSO/PSO regarding additional government customer and agency reporting requirements.

For additional information, click [here](#).

Reportable Activity for Secret

- Foreign Contacts (Official & Unofficial)
- Behavior & Conduct (Attempted elicitation, exploitation, blackmail coercion or enticement)
- Foreign Affiliation; application for or receipt of foreign citizenship
- Media Contact
- Criminal Activity
- Counseling and Treatment
- Personal Finance and Business Interests
- Foreign Travel (Unofficial), deviations from submitted travel itinerary, unplanned trips to Canada or Mexico, emergency circumstances.

Reportable Activity for Top Secret & SCI

- Foreign Contacts (Official & Unofficial)
- Behavior & Conduct (Attempted elicitation, exploitation, blackmail coercion or enticement)
- Foreign Affiliation; application for or receipt of foreign citizenship
- Media Contact
- Criminal Activity
- Counseling and Treatment
- Personal Finance and Business Interests
- Foreign Affiliation; voting in a foreign election
- Personnel Finance & Business Anomalies; financial anomalies, direct involvement in financial business, foreign bank accounts, ownership of foreign properties
- Living Status/Arrangements; cohabitation, marriage, adoption of non-U.S. citizen children, foreign national roommates
- Foreign Travel (Unofficial), deviations from submitted travel itinerary, unplanned trips to Canada or Mexico, emergency circumstances.

Who Should Report

Everyone has a duty to report. Reports should be based on facts and not rumor or gossip.

How to Report

Report all activity about yourself or others to your local FSO/PSO.

Any suspicious activity whether in the classified or unclassified environment should be immediately reported to the Counterintelligence & Threat Management program/Insider Threat Program Senior Official (ITPSO) at CITM@saic.com. *For additional guidance on suspicious reporting, refer to the section of this training on Counterintelligence and Operational Security.*

Employees who hold active security clearances are required to report all international travel, including personal trips. Employees should use the International Travel Request System (ITRS) to submit their itinerary, which will be kept on file for reinvestigation purposes. *For additional guidance on reporting international travel, refer to the section of this training on International Trade Compliance & Crisis Management.*

What Does SAIC Security Do With the Information I Report

SAIC Security has an obligation to report items that may have an impact on your security clearance to the U.S. Government via the system of record. Security will only report facts, not hearsay. Unless something is reported that has an impact on SAIC or is deemed to be a threat to a person or persons at SAIC, the reporting stays between you and SAIC Security. If a valid adverse security violation has occurred, the appropriate leadership will be informed.

Safeguarding Information

Classified Information Security

It is every employee's responsibility to protect customer information they are entrusted with. Those with a clearance and who have access to classified information, have a heightened responsibility.

Handling Classified Information

When handling classified information it is important to abide by customer and SAIC security guidelines. Protect classified information and prevent possible inadvertent disclosure by taking the following precautions.

Step 1. Mark Documents Correctly

Ensure all documents are marked correctly and use cover sheets for all classified documents.

Step 2. Destroy Unneeded Information

Always follow proper destruction guidelines when information is no longer needed; it is your responsibility to ensure classified material is handled accordingly. At the end of the contract, information is either destroyed or returned to the customer.

Step 3. Secure Hand Carried Information

When hand-carrying classified information, ensure you have been properly briefed and the materials are secured appropriately.

Step 4. Handle Media Appropriately

Classified information shared in the Media does not indicate that it's been declassified. Never confirm, deny, or validate information seen in the public domain.

Step 5. Store Material Properly

Leaving for the day? Store classified and unclassified materials appropriately based on the approved storage requirements of your facility.

Collect documents from the printer as soon as they are printed. Don't forget to pick up originals from the copier or fax machine.

Pre-Publication Review

All written and oral materials to be published or presented must be submitted to the Government for review and approval prior to release. Written and oral materials may include the following:

- Speeches
- Articles
- Web pages, web sites, blogs
- Resumes, Biographies
- Books, Memoirs, Literature (including fiction)

Plan Accordingly

Most agencies have 30 days to respond. If you are briefed through more than one customer, EACH customer may need to review prior to release.

Data Spillage

Data 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. Data spills are a serious concern and must be **reported** immediately.

Any actual or suspicion of data spill, malicious code, or virus on your computer must be reported immediately to your FSO/PSO and ISSM.

Security Violations

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
- Mishandling classified material
- Improper marking of classified information
- Improper disclosure of classified information
- Failure to report personnel security reportable matters

Be Aware: Sending CUI to personal email accounts is strictly prohibited and will result in disciplinary action. As such, SAIC has established a "graduated scale of disciplinary actions" for employee violations of security regulations or negligence. Please view the **SAIC Standard Practice and Procedures** for more details

Please be advised that the unauthorized **disclosure** of classified information may result in **criminal, civil, and administrative penalties**, even though an individual has not yet signed an NDA (Reference: 32 CFR 117.12(e)(6)). Furthermore, SAIC Security is responsible for the **prompt reporting** of information to the government Cognizant Security Agency that may question the trustworthiness or reliability of an employee. As such, SAIC has established a "**graduated scale of disciplinary actions**" for employee violations of security regulations or negligence. Please view the **SAIC Standard Practice and Procedures** for more details.

Classification Management

Classification Management involves the identification, marking, safeguarding, declassification, and destruction of classified national security information generated by the Government and Industry. It encompasses the life-cycle management of classified information from original classification to declassification.

Classification Levels

The U.S. Government applies three (3) levels of classification protection. [Executive order 13526](#) established the criteria for classification and protection of national security information.

Levels of Classification

- **Top Secret:** Unauthorized disclosure can cause **exceptionally grave damage** to national security
- **Secret:** Unauthorized disclosure can cause **serious damage** to national security.
- **Confidential:** Unauthorized disclosure can cause **damage** to national security.

Types of Classifiers

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

Derivative Classifier: Is given the authority to incorporate, paraphrase, restate, or generate a new form of information that is **already** classified.

SAIC employees who **generate** classified materials are Derivative Classifiers.

Derivative Classified Responsibility

If you are a Derivative Classifier, you are to self-identify and carry forward instructions for classification and markings from sources, customers' instructions and/or classification guidance.

It is also your **responsibility** to challenge and seek clarification for incorrect or incomplete markings on Derivative Classified materials. The formal challenge must be in writing to an OCA. The agency shall provide an initial written response to a challenge within 60 days.

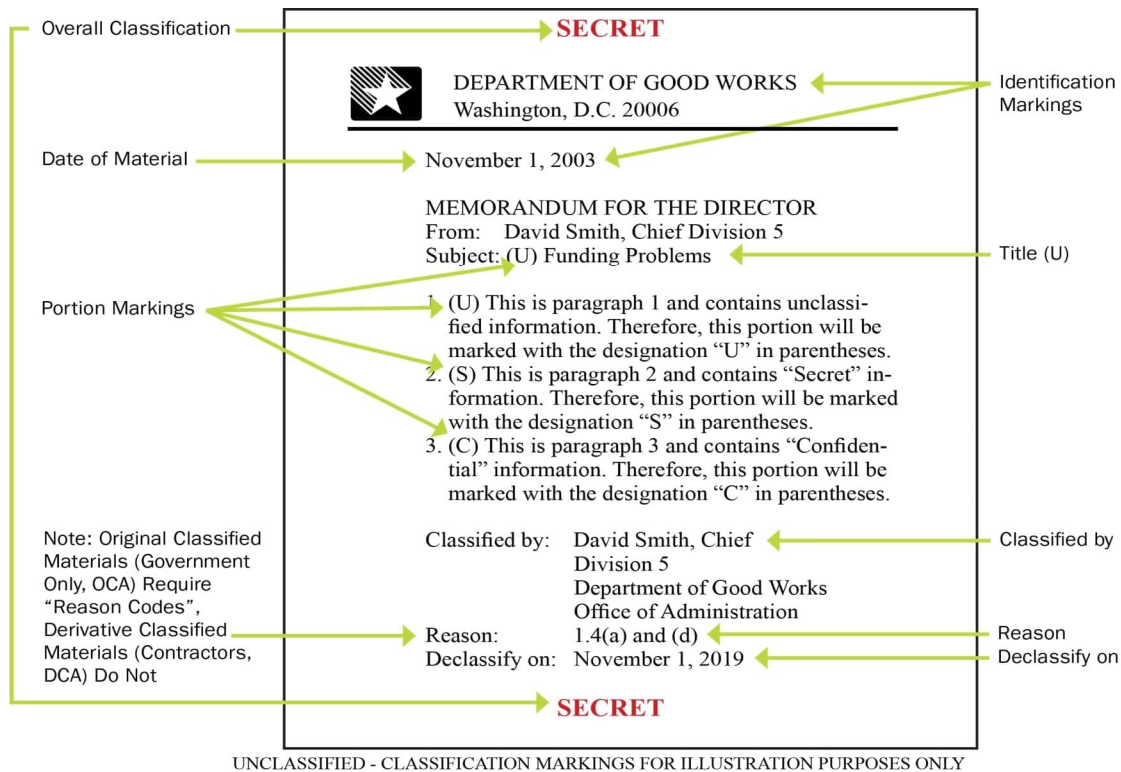
Never originally apply classification markings, downgrade classified information, guess or assume classification levels, or provide "subject matter expertise" or classification guidance to any source unless authorized by an OCA or classification guide.

Classification Marking

Classification portion marking is used to identify and protect classified information by:

- Facilitating the sharing of information among agencies
- Distinguishing different classification levels within a document
- Aiding in future review and release of documents

All materials, including media, are required to have the following identification markings.



Classification Banner Markings – All documents must contain the Classified banner markings to include Identification markings, date of material and title(s).

Portion Markings – Indicates the classification of material contained in the document.

Reason for Classification – Reason for classification is required for original classification

Classified By – Indicates either the original or derivative

Derived From – Required only for derivative classified information

Declassification – Declassification instructions

Working Papers

Working Papers remain classified from their **date of origination** per SAIC guidelines. Different classifications require different lengths of time.

- **Confidential** - 180 days
- **Secret** – 180 days
- **Top Secret** – 30 days

After these time periods, they are either destroyed or placed into the accountability system, depending on facility requirement.

Prohibitions, Limitations, and Sanctions

When classifying documents as a **Derivative Classifier**, there are prohibitions, limitations, and sanctions you must keep in mind.

Prohibitions

- Avoid over-classification
- Do not "**strip**" classified information to create unclassified materials (**without Government Contracting Activity review**)
- Do not "**talk around**" classified information with unclassified terms to relay information in a non-secure area

When a document reaches its declassification date, determinations for re-classification or public release are made at the OCA level.

Refer all questions to your local program office.

Limitations

- It must be determined, **in writing**, that re-classification of the information is necessary in the interest of National Security
- Material must be **reasonably recoverable**
- Classification must be reported to Information Security Oversight Office **within 30 days**
- Reclassified information must be appropriately **marked** and **safeguarded**

Sanctions

There are stiff **penalties** for mishandling or disclosing classified information:

- Reprimand
- Suspension without pay
- Program removal
- Termination of classification authority
- Loss or denial of access to classified information
- Other sanctions in accordance with applicable law and agency regulations

USE CAUTION: Compilation of unclassified facts could make the information classified.

When in doubt, consult your customer or security classification guide for guidance.

Safeguarding Classified Information

You must protect both classified and unclassified information at all times. Use caution when revealing details regarding the following to those without a Need to Know:

- Program name(s)
- Technology
- Program Mission
- Locations
- Costs
- Research and development activities

Physical Security

Physical security measures are taken to prevent unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm.

Security Badges

Badges are issued as a physical security control to identify authorized personnel. Employee badges control access to those facilities and areas you are authorized to access.

To protect SAIC employees and property follow these simple rules:

- Wear your badge visibly at all times when while on company premises.
- Secure your badge when not on company premises. A lost badge can compromise SAIC security.
- If you lose or misplace your badge, contact the local security representative as soon as possible.
- Challenge anyone without an SAIC badge on SAIC premises and report to your local security representative immediately.

Identify that Badge!

SAIC employee badges are vertical and non-employee badges are horizontal.

EMPLOYEE BADGE TYPES



Uncleared Employee



Foreign National



Permanent Resident

NON-EMPLOYEE BADGE TYPES



Foreign National Contractor



Permanent Resident Contractor *



Contractor Uncleared



Government Uncleared

Prohibited Items at SAIC

The following items are prohibited at SAIC facilities:

- Firearms, or any other item that may be used to inflict bodily harm or threaten and/or intimidate others.
- Explosive or incendiary devices.
- Controlled substances, including illegal drugs and paraphernalia; except prescription medicine.
- Surveillance equipment, cameras, or audio/video recording equipment.
- Other items prohibited by law.

Visitor Facility Access

All visitors must be signed in or registered by the sponsoring employee and are the responsibility of the sponsor throughout the visit.

Foreign Nationals:

- Foreign National visitors must be approved prior to entry into SAIC cleared facilities. Requests are approved by SAIC Security and the International Trade Compliance (ITC) office.
- Coordinate early with SAIC Security and ITC for non-U.S. Persons visits.
- All Foreign National visitors must be escorted at all times.

Controlled Spaces

There are four types of controlled spaces at SAIC that are approved for **storage**, **discussions**, and **processing information** of different clearance levels.

Holding a clearance does not mean you are cleared to access these spaces. Access is limited to **authorized persons** who have an appropriate security clearance and a need-to-know for the classified matter within each specific area.

Additionally, for unclassified spaces and controlled spaces, tailgating is prohibited. Every person must individually badge into any space that has a card reader.

Learn More About the Controlled Spaces Below:

- **Restricted Areas:** Designated for the handling of information up to the Top Secret level. Storage is not permitted.
- **Closed Areas:** Used for the handling of information up to the Top Secret level.
- **Sensitive Compartmented Information Facilities (SCIFs):** Designated for handling information at the SCI level.

- **Special Access Program Facilities (SAPFs):** Used for handling SAP level information and have been modified to prevent sound from leaving the space.

Prohibited Items Within Controlled Spaces

A **Personally-owned Portable Electronic Device (PPED)** is not permitted within controlled spaces. A PPED is a device capable of **recording, storing, and/or transmitting data**, voice, video, or photo images, such as your smart phone.

PPEDs pose a risk to the confidentiality, integrity, and availability of customer information. It is your responsibility to know what technologies you have on you.

If you are prescribed a Medical Portable Electronic Device (MPED) please contact your local SAIC FSO/PSO to help coordinate approval.

Classified Meetings

If you are hosting a **classified meeting** at a cleared SAIC facility, you must:

- **Coordinate** specifics with your local **SAIC FSO/PSO** as early as possible, but no later than 5 business days prior to the meeting.
- Ensure **individuals** in attendance have a **Need-to-Know** and clearances have been received.
- Establish the **security level** of the meeting.
- **Report** any **foreign nationals** to SAIC Security and Export Control (International Trade Compliance) for approval prior to visiting an SAIC facility. Foreign nationals that try to substitute for another foreign national visitor will not be authorized access to the facility.
- Know the **approvals** in place for the **conference room** you are using.
- Know what **network requirements** are needed for the meeting (Accreditation levels for rooms can vary. Some spaces may be accredited for discussion only, and some for discussion and processing. Approved storage procedures could also be different for each site)

Immediately report any real or suspected security instances or violations to SAIC Security.

SECTION 6: COUNTERINTELLIGENCE

Recognizing Threats

Counterintelligence is about **identifying** the threats, developing strategies to **mitigate** those threats, and taking action to **counter** adversary intelligence, espionage and sabotage efforts.

The counterintelligence examples below are actions we take to protect classified and sensitive information.

- Report Odd Behavior
- Know the Targets
- Know the Adversaries
- Protect and Report Information

External Threats

Unlike Insider Threats discussed earlier, external threats are more broad reaching and organized.

Foreign Intelligence Services (FIS) Can come from non-ally countries and our own ally countries.	Foreign & Domestic Industry Competitors Will commit industrial espionage to gain information to gain a competitive edge.	Criminal Activist & Terrorist Organizations Look to obtain information that seeks to further a cause vs. gaining an edge.
--	--	---

Collection Methods

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.

There are several methods that external threats use to collect information for Methods of Operation.

Methods of Contact: The approach used to connect the foreign actor to the targeted individual, information, network or technology in order for the foreign actor to gain access to information of value.

Academic Solicitation: Someone requests to study or consult with faculty members, or applies for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows or employees.

Request for Information: Requesting information is the most frequently reported collection method and provides the greatest return for minimal investment and risk. Collectors use direct and indirect requests for information (email, phone calls, conversations) in their attempts to

obtain valuable U.S. data. A simple request can gain a piece of information helpful in uncovering a larger set of facts.

Solicitation of Marketing of Services: Foreign-owned companies market their services to U.S. firms. Their intention is to seek business relationships that enable them to gain access to sensitive or classified information, technologies or projects.

Acquisition of Technology: Collectors attempt to acquire technology and information through third parties, using front companies, and directly purchasing U.S. firms and technologies.

Official Foreign Visitors & Exploitation of Joint Research: Foreign government organizations, including intelligence and security services, consistently target and collect information through official contacts and visits.

Public Venues: Conferences, conventions, symposiums, and trade shows offer opportunities for foreign adversaries to gain access to U.S. information and experts in dual-use and sensitive technologies.

Cyber Attack: Cyber threats are increasingly persistent and rapidly becoming a primary means of obtaining economic and technical information. Cyber attacks against the U.S. government and business entities continue to increase. Adversaries have expanded their computer network operations and the use of new venues for intrusions has increased.

Mobile Telephones: Smart phones and other devices are susceptible to malicious software.

Foreign Targeting of U.S. Travelers Overseas: Collectors can elicit information from U.S. travelers via seemingly harmless conversations, eavesdropping on telephone conversations, overhearing conversations in public settings, and downloading information from laptops.

Targeted Information and Sectors: Foreign collectors continue to seek a wide range of unclassified and classified information and technologies from specific targets. Information systems attract the most attention; aeronautics, lasers and optics, sensors, and marine systems are among the top targets.

Operations Security (OPSEC)

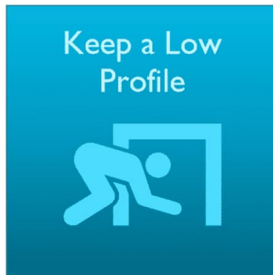
OPSEC is an analytic process used to deny an adversary information, generally unclassified, concerning friendly intentions and capabilities by **identifying, controlling,** and **protecting** indicators associated with planning processes or operations.

OPSEC Process - The OPSEC Process consists of **five (5) steps**. These steps help to identify information requiring protection, determine the methods that may be employed to compromise that information, and establish effective countermeasures to protect it.



OPSEC Countermeasures

Collection threats come from many places (i.e., foreign governments, competitors, and even coworkers). We must use **Counterintelligence** to counter adversarial intelligence, espionage and sabotage efforts. An **OPSEC indicator** is any piece of information that can be exploited to gain further information or combined with other indicators to build a more complete profile of your operation. Protect your OPSEC indicators by practicing the following countermeasures:



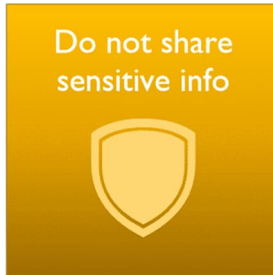
- Don't "advertise" your presence or your work on social media sites
- Don't wear contractor/customer badges in public



- Be aware of the surroundings (environment/threats)
- Recognize when something is wrong



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



- Identify, control, and protects sensitive unclassified information
- Protecting sensitive information reduces vulnerabilities

Other Security Concerns

Criminals and hackers are constantly coming up with new and sophisticated schemes to compromise computers, networks, valuable information, and passwords. Let's explore the many threats you must watch out for both at work and in your personal life.

Security Threats

Technical

- Phishing
- Ransomware

Non-Technical

- Vishing - Similar to Phishing, except telephones are used in an attempt to obtain private information that will be used for identity theft.
- Social Engineering - Someone attempting to persuade another person to break normal security procedures in order to gain inside information.
- Impersonation - An impersonator poses 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 attack.

Internet Security

Anyone accessing SAIC systems and data is subject to **monitoring** and must adhere to the **Acceptable Use of SAIC Information Systems and Assets Policy**.

Your use of the SAIC internet connection is **traceable**. Conduct any activities such as internet searches, news group posts, chat room dialogue, remote logins, etc. with SAIC's **reputation** and your **cleared** status in mind.

Although a variety of internet sites support SAIC business purposes, others are inappropriate to access using SAIC systems.

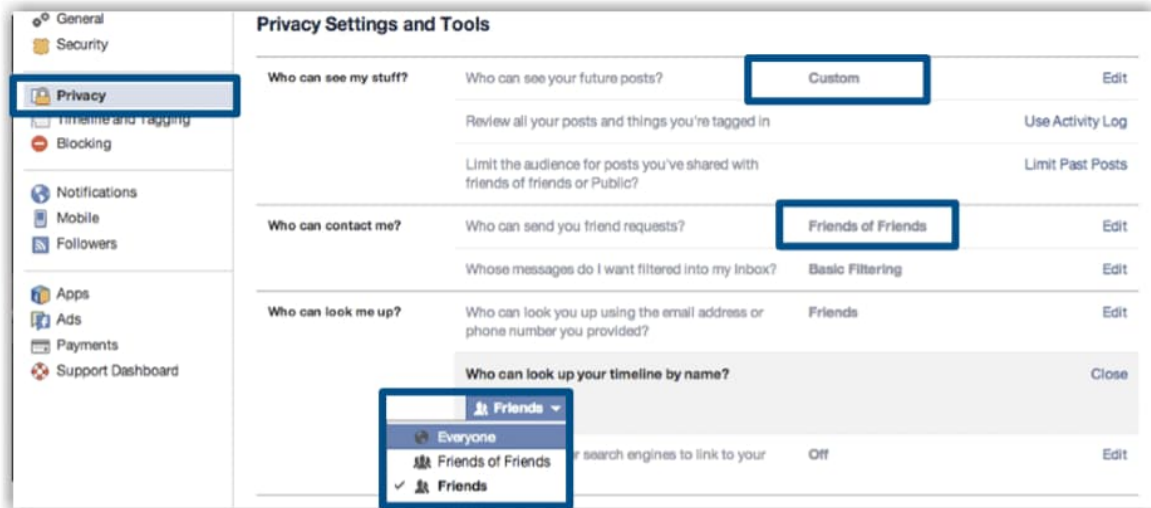
Inappropriate sites and searches include:

- Sexually explicit and graphically inappropriate
- Promoting racism or bigotry
- Conflicting with company policies or and interests
- Infringing on intellectual property rights

Social Media

Social networking sites are a great way to connect and share information. However, the amount of visitors these sites attract makes them extremely vulnerable to cyber criminals.

Review your privacy settings **routinely** and be **cautious** of what you reveal in online forums, to include customer and SAIC proprietary information.



Counterintelligence Reporting Requirements

The keys to successful counterintelligence or insider threat mitigation are rapid detection and reporting a potential threat – real or perceived.

Reporting Counterintelligence Threats

The following **MUST** be reported to **SAIC Security (FSO/PSO)** and **Counterintelligence & Threat Management**:

- All foreign travel or contact with foreign contacts (must be reported to the Customer as well)
- Contact with anyone or information that suggests SAIC personnel may be the target of intelligence collection
- Contact with a known or suspected Intelligence Officer (IO)
- Requests by anyone for unauthorized access to SAIC sensitive information or customer information
- Actual or attempted unauthorized access to SAIC or customer IT systems
- Someone asking for information beyond what is publicly available
- Suspected attempts of cyber elicitation or suspected receipt of malicious code
- Suspicious behavior in the workplace

If you are unsure whether or not to report something - report it! Better to report, investigate, and discover it is innocuous than not to report and suffer a potential loss of personnel, information, or resources.

Reporting Channels

- Security via **email**: (CITM@saic.com)
- **Suspicious Reporting Tool** in ES3
- Reporting **Helpline** (888-247-1764)
- **Online** submission (<https://saicintegrity.com/>)

Anonymous reporting is available via the “Reporting Helpline” and/or the “Online Submission” channels.

If you are unsure – REPORT IT anyway!