ANNUAL SECURITY REINDOCTRINATION (ASR) DESK REFERENCE

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

January 2026

Security Awareness Training & Education (SATE)
SATE-Team@saic.com

SAIC®

Table of Contents

SAIC®

Introduction

The National Industrial Security Program requires that employees receive security training to include an initial security briefing before being granted access to classified information as well as annual refresher training.

Security training is more than just a requirement; it's also an opportunity to empower ourselves with the tools and awareness necessary to navigate and protect SAIC's information. Thank you for your continued dedication to security excellence.

If you have any questions, please direct them to the Security Awareness Traning & Education team at SATE-Team@saic.com.

Let's Get Started

In your SAIC role, you may handle sensitive information from SAIC, customers, or third parties (e.g., subcontractors). Protecting this information is essential. This first module covers Data and Information Security and Protections.

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
• 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	• 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

Remember, all sensitive data must be properly protected. Misuse of material information may be a violation of the Securities and Exchange Act with accompanying penalties of civil and/or criminal fines as well as imprisonment.

All employees are subject to the company's insider trading policy (SI-POL1-04), which prohibits trading in SAIC stock while in possession of material non-public information.

Please review the policy now to familiarize yourself with these rules and complete the attestation below.

Sharing Information Safely

Data and File Sharing Protections

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

Always Ask "Why?"

When you receive a request for sensitive information from someone who is either not authorized or who does not have a need to use the information, the first question you should ask the requestor should always be "Why?" What justification can the requestor provide as to why that information is needed? Consider if something less can be provided in order to accomplish the task at hand. If the requestor insists that they be provided sensitive information, please reach out to the Legal Office or the Chief Privacy Officer for guidance.

Encryption

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

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

SAIC preferred and approved methods of encryption for sending information outside of the SAIC network:

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

** PIV: Personal Identity Verification/CAC: Common Access Card*

Certain types of data shared within SAIC email to another SAIC employee within SAIC email require additional protection based on the category of data and the intended recipients of the email.

When sending email, be aware of the following types of sensitive information and ensure proper encryption:

Within saic.com email to saic.com address, encrypt with certificates or through SFTP:

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

From within saic.com email to appropriate external address after determination to receive such information is obtained:

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

Email to external email addresses should only be sent to appropriate customer or subcontractor/prime email accounts. NEVER send encrypted email or any sensitive information to personal email addresses (e.g. gmail, Outlook, Hotmail).

Collaboration Tools

SAIC offers various collaboration tools to conduct business and collaborate. These tools are designed to facilitate secure meetings, file transfers, and real-time communication.

Things to remember when using collaboration tools:

- Communication shall remain professional and must not contain any material that may reasonably be considered offensive, disruptive, defamatory or disparaging.
- There is no expectation of privacy when using SAIC collaboration tools.

Recording and Transcription Policy

- Recording and transcription features are available but are subject to limitations. Please be mindful of the following:
- Access to recording, transcription, and intelligent recap options will be granted only after completing the necessary training and are authorized solely for legitimate business purposes.
- Meeting hosts must inform participants at the start that the meeting is being recorded, transcribed, and/or recapped so they can provide informed consent.
- Recording, transcription, and recaps must be protected from unauthorized disclosure, stored in SAIC's secure environments, and shared with non-SAIC participants only with legal department approval.
- Meetings involving highly sensitive information, where consent from all participants hasn't been obtained, or where prohibited by customer contracts or agency policies, should not be recorded, transcribed, or recapped.

For more guidance on recording and transcription, please see SI-POL1-12 (Acceptable Use Policy)(opens in a new tab) and SI_POL04-6 (Records and Retention Instruction).

Collaboration with Customers

There may be additional security requirements when using collaboration tools to interact with customers. For example, DoD customers may require video/audio meetings to discuss CUI be hosted on a tool that meets DoD Impact Level 4 (IL4) protections. Prior to customer meetings, confirm tool compliance with customer security requirements via ISSAIC or contact Tell.IT@SAIC.com for guidance.

Anytime you discuss CUI during a recorded or transcribed meeting, you are creating CUI records that need to be adequately marked and protected.

Reminder: Understanding the risks associated with file sharing and data privacy is critical. It is each employee's responsibility to use SAIC's collaboration tools in compliance with our policies, ensuring data integrity and security.

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

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

Safeguarding Sensitive Information and Data

Senstivie Data Precautions

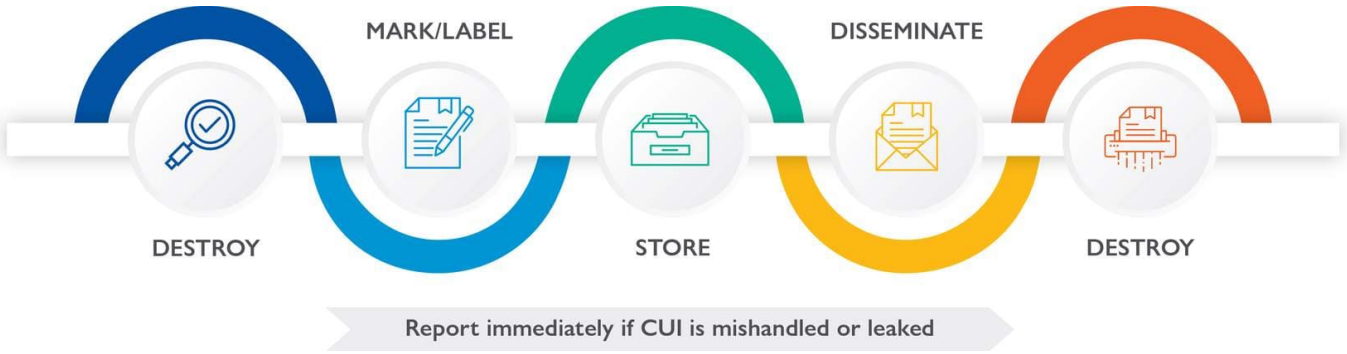
Information and data are the lifeblood of SAIC and our customer's business. We must be Guardians of all information and data. It is critical you are aware of how to identify, store, and properly disseminate sensitive information.

In the next lessons, you'll learn more about the different types of sensitive data.

Controlled Unclassified Information

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



Be Aware:

Report it immediately if CUI is mishandled or leaked. For more information, please see SAIC's Information Systems Security Protection Policy (SI-POL1-09).

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

What CUI is not:

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

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

CUI markings cannot be used to:

- Conceal violations of the law, inefficiencies, 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

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. Documents and data created by SAIC shall be properly marked as CUI in accordance with contract requirements. Employees should avoid marking items that do not require CUI labeling per their contract. Check with your program manager if you need assistance with labeling.

Required CUI markings include:

- Header/top/banner of the document must have CUI or CONTROLLED in bold letters
- Designation Indicator Box shall be located on the Cover Page and/or Title Page and must include the following:
  - Who owns the information
  - Who controls the information
  - CUI category contained in the document (CTI, OPSEC, etc.)
  - Distribution Statement/Limited Dissemination Control (LDC) information
  - Main contact or POC

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.

STORE

System Storage

The NIST SP800-171 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 resaonable 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.

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.

SAIC

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, up to and including termination. 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.

If you have questions or need further information regarding CUI and proper handling, please reach out to the CUI Program

Other Protected Data

Personal Information (PII/PHI)

SAIC employees often work with or are exposed to personally identifiable information as part of our work with government customers or internally at SAIC. This information requires protection. Let's look at each type and how to protect it. See below:

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
- Date 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

Peronal 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.
- Add an extra layer of security by encrypting PII/PHI when sending and only use SAIC's SFTP for transmission. Please reach out to the CISO's office (cybersecurity_grc@saic.com) FIRST if alternative transmission means are needed.

Always ask "WHY?" when receiving a request to provide PII/PHI. DO NOT share PII/PHI with those NOT AUTHORIZED to use &/or view the data. DO NOT share unredacted PII/PHI externally without first reaching out to the Privacy Office for approval.

Proper Data Storage

Cloud Storage Usage

To protect our sensitive data, adhere to the following guidelines:

1. Only Use Approved Cloud Services: Only use cloud storage solutions that have been explicitly approved by SAIC Cybersecurity for storing SAIC or customer data.
2. Understand Customer Requirements: Ensure compliance with additional customer protection requirements before using any cloud solution.

Storing sensitive data improperly can lead to severe penalties and legal actions. Always use approved, secure methods for data storage to comply with SAIC and customer requirements.

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

Physical Data Protection and Destruction Considerations

We must continue to protect data when it is in physical form on paper. 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 top or anywhere outside of full bins. Store in a locked cabinet until a bin is available.
- Understand the requirements of your customer/contract for data storage and destruction.

SAIC policy (SI-POL1-09 and SI-POL1-12) states that employees must only print SAIC and customer data on a printer managed by SAIC and NEVER to a personal printer.

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

Artificial Intelligence (AI) Technologies and Protected Email Use

Artificial Intelligence (AI) Technologies

Always Exercise Caution

Be mindful of what you enter into AI tools and make sure inputs are in line with SAIC policies and instructions before submitting.

Things to remember when using AI technologies

1. Do not enter SAIC or customer sensitive, proprietary, or personal data into AI technologies not approved by SAIC for that specific use.
2. Ensure you are familiar with your contract requirements and customer's policies regarding the use of AI, and obtain appropriate written authorization prior to use.
3. Always evaluate the output of any data or information for appropriateness, accuracy and validity. *AI outputs are not always factual and may include hallucinations. This is one of the primary risks facing AI users and makes evaluating outputs a critical component of using AI.*
4. Remain aware of any SAIC policies and guidance regarding AI by reviewing the AI page on ISSAIC

Remember that AI use must be in compliance with SI-POL1-12 (Acceptable Use of SAIC Information Systems and Assets), SI-POL-05 (Data Privacy and Protection), SI-CYBER-03 (Artificial Intelligence Instruction), SI-POL1-09 (Information Systems Security Protection), and SI-POL1-08 (Intellectual Property).

It is prohibited to input or send proprietary or sensitive information, including Controlled Unclassified Information (CUI), through ANY non-approved systems, including AI tools. By using AI properly, we keep data safe and safeguard privacy.

Protected Email Use

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.

Email notifications such as SAIC Now, other corporate News/updates, and messaging from leadership may contain company sensitive information. These messages shall not be forwarded to non-SAIC email accounts.

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:

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

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

Cybersecurity and Insider Threat

Cybercrime Concerns

Be Aware of Cybercrime

SAIC employees are targeted by cybercriminals due to our government work and access to national security information. These hackers aim to exploit and steal valuable data.

Phishing

Phishing is a daily threat to SAIC. Attacks are carried out through fake emails, websites, text messages, and phone calls to target our employees. Learn more by examining each numbered indicator below.

1. Verify the Sender: Verify the sender is someone you know and is using a valid email address. it@verifypass.pw is not a valid SAIC email address.
2. Proceed with Caution When You See an External Sender: SAIC has configured your inbox to label all external emails with a red warning. This warning is your cue to read external emails very carefully before acting.
3. 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.
4. Don't Skim an Email Just Becaue it Looks Ordinary: Attackers try to take advantage of common, real-world scenarios and activities to lend to create false credibility. Common uses are password changes, invoices, shipment notifications, and offers for marketing lists.
5. 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 will take you. Additionally, consider if this process seems in line with our company processes and policies.
6. 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?

You can easily report suspicious email via SAIC's email system.

How to Report Suspicious Email: Report suspicious emails immediately by using the Phish Alert button in Outlook, or send an email to L_Report_Phishing@SAIC.COM with the suspicious email as an attachment.

Ransomware

Ransomware is another means to steal sensitive data. Ransomware encrypts systems to block access until a ransom is paid, often threatening to release captured data. It typically spreads via email but can also spread using PDFs, thumb drives, apps, or other social engineering tactics that infect the computer system and bypass the firewall.

The availability of numerous ransomware tool kits for sale online has made launching these attacks even easier and more prevalent. Attackers often target large companies with sensitive data, like SAIC.

Protect Yourself and SAIC

Always maintain multiple copies of your most essential data to safeguard business continuity in the event of a ransomware attack. Consider storing one copy in an access controlled SAIC SharePoint or Teams group.

- Be on the Lookout For:
- Unexpected invoices from vendors
- Unprompted account password change requests
- Seemingly random package delivery attempt notifications
- Credit card activity notices you don't recognize

Be Aware: If you receive a threatening message demanding payment, disconnect your system from the network and call 833-YOCYBER right away.

Social Media and Cybercrime Risks

Social networking sites are powerful tools for connection and share information. However, these sites are also extremely vulnerable to cyber criminals.

Bad actors use social media sites, like LinkedIn, to gather information. Be cautious about what you post and the connections you make. Review your privacy settings regularly and be cautious of what you reveal online. Do not reveal any sensitive customer or company information.

Key Concerns:

- Information Gathering: Cyber criminals use platforms like LinkedIn to collect information for attacks. Be extremely cautious about the details you share.
- Connections: Scrutinize connection requests and only accept those from trusted sources.
- Privacy Settings: Regularly review and update your privacy settings to control who can see your information.
- Information Disclosure: Avoid posting sensitive information related to the company or customers in online forums or social media.

Best Practices:

- Limit Sharing: Share minimal personal and professional information.
- Verify Connections: Confirm the identity of individuals before accepting connection requests.
- Use Strong Privacy Settings: Ensure that your privacy settings are set to the highest security.
- Be Observant: Watch for suspicious activities or requests that seem unusual or inappropriate.
- Policy Adherence: Follow company policies regarding social media and information sharing.

By following these guidelines, you can help protect yourself and the company from potential cyber threats originating from social media platforms.

Public Computer Usage:

SAIC strictly prohibits the use of public computers (e.g., kiosks, hotels, etc.) to access SAIC systems due to high cyber risk. They are prime targets for cyber criminals and may be compromised. Only use SAIC-approved devices to access SAIC Information Systems and ensure the protection of our sensitive data.

Insider Threat

Insider threats come from persons who have/had authorized, 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 motivations is "CRIME".

Coercion
Coercion is defined as being forced or intimidated.

Revenge
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.

SAIC

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 or obtains 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

Peronal 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

Remain aware of your surroundings and speak up when something does not seem right.

- Suspicious activities or persons - *people or events in or around facilities that appear unusual*
- Facility safety problems - *unsafe building operations, malfunctions, or hazards*
- Crime - *property or violent crimes*
- Workplace disruption - *employees exhibiting behavior that may harm themselves or those around them*

Suspicious Behaviors

Every SAIC employee has a responsibility to report suspicious behaviors. You can submit a report via the Security page on ISSAIC or via saicintegrity.com or 888-247-1764.

- *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

It is important to remain aware of your environment and unusual behavior. As an SAIC employee, you have a responsibility to speak up when something does not seem right. Remember, concerns can be reported via the Security page on ISSAIC.

Doing Your Part

Your role in the Insider Threat Security process has three parts:

- Follow SAIC policy and guidance
- Be alert and aware in your daily activities – use good judgement when working with SAIC information and systems
- Report anything suspicious or out of the ordinary

Remember, you are an integral part of SAIC's Security Solution. Report anything suspicious!

Securing SAIC Assets

Protected Hardware Use

Use Assets Wisely

The Acceptable Use Policy, SI-POL1-12, 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.

Guardian Basic: You cannot take your SAIC laptop outside the U.S. without prior authorized permission from SAIC Cybersecurity and the International Trade Compliance (ITC) team.

Mobile Devices

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

- Ensure compliance with SI-ITS-04 prior to installing SAIC-approved mobile apps on personal devices.
- Do not conduct SAIC business on personal devices outside of SAIC-approved mobile apps.
- Do not conduct SAIC business using personal text messaging or ephemeral messaging services (e.g. Signal, Telegram, WhatsApp).
- Do not share sensitive SAIC or customer data via text or unencrypted email on your personal device.
- Maintain positive control of your device at all times.
- Do not let unauthorized personnel view customer or SAIC data on the device.

Guardian Basic: 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 OR 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.

Guardian Basic: 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 remotely, 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
- Connecting any SAIC asset to a printer **not issued or managed by SAIC**

What are Your 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

Be Aware: Check out SI-POL1-12, the SAIC Acceptable Use Policy, on ISSAIC for more information. Violations of the Acceptable Use policy carry significant consequences up to and including termination.

International Trade Compliance & Crisis Management

International Trade

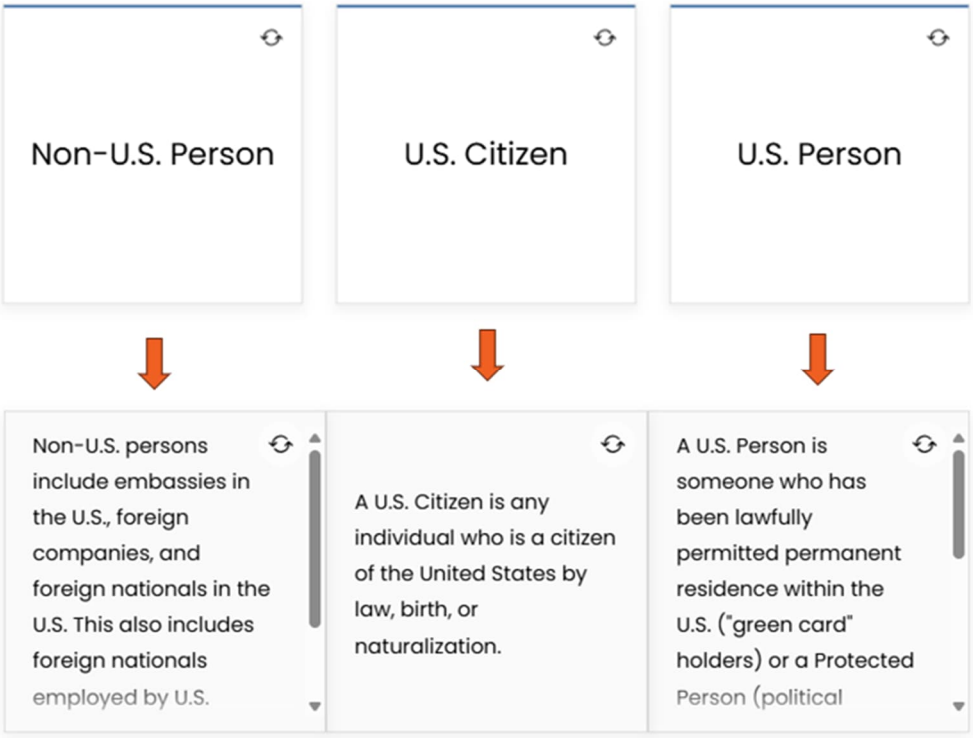
International Trade Compliance

The U.S. Government has complex regulations for the import, export, and release of certain products, services, and technical data to a foreign person or foreign entity. 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 (ITC) in advance of any of the following:

- Discussions where a foreign national will be in attendance (including foreign nationals visiting the U.S.)
- Exporting Technical data, hardware, or software
- International travel
- Imports of controlled goods

Import and Export Compliance

Understanding the Players



SAIC email address display names indicate the citizenship status of each employee. Be aware of this status in order to avoid sending information or data to non-U.S. Persons via email without proper approval. Sending controlled information to a non-U.S. Person without authorization in place is illegal exporting, and could be subject to fines and/or imprisonment under the law.

Status	Example of SAIC Email Address Display Name
Non-U.S. Person	Doe, Jane Non-US
U.S. Citizen	Doe, Jane US
U.S. Person	Doe, Jane USP

Note: SAIC Non-Employees have the same display name indicators based on their legal status within the United States along with "_CTR" following their display name to signify their non-employee status.

Import/Export Regulations

International Traffic in Arms Regulations (ITAR)

The ITAR controls highly sensitive defense articles, services, and technical data. ITAR-controlled items can be found on the U.S. Munitions List (USML) and require an export authorization.

ITAR:

- Regulated through the State Department's Directorate of Defense Trade Controls
- Controls highly sensitive defense articles, services, and technical data
- Requires an export authorization

Technical Data Transfer also includes training and presentations.

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.

EAR:

- Commercial items: 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.
- ITC Permission Required: 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.

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

Export and import compliance is complicated. Reach out to ITC early for assistance. If you are unsure if your program will engage foreign nationals in the U.S. or while supporting overseas operations, check with your supervisor.

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 or Import 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.

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

Import and Export Authorizations

The Approval Request for Imports and Exports System (ARIES) is a tool used by SAIC employees to request ITC approval for all imports and exports of USML controlled goods. 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.

Click here to access the ARIES page on ISSAIC.

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

Possible USML or Other Controlled Imports May Include:

- Firearms
- Ammunition
- Temporary imports of anything controlled
- Military software designed for military use

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.

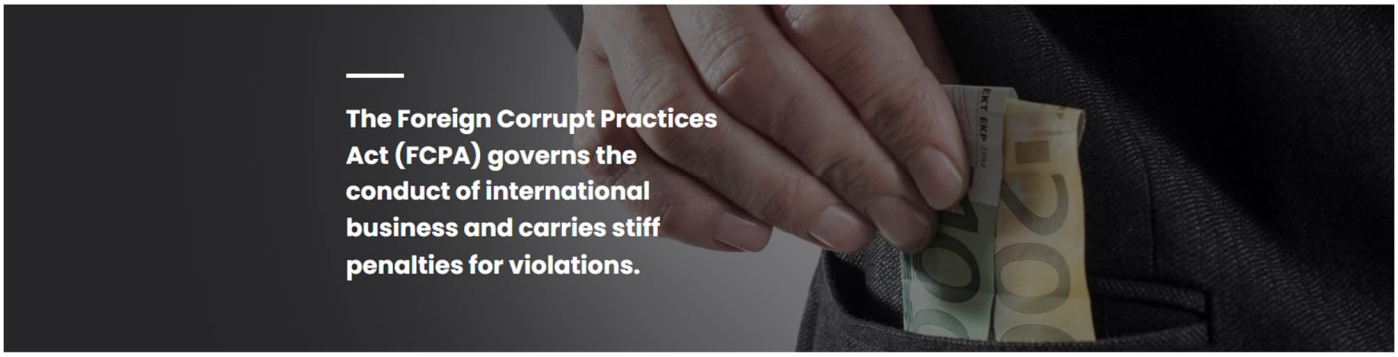
You must have an approved export license, agreement, or exemption in place for the following:

- Exporting commodities
- Providing defense services
- Exporting controlled technical data

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

International Business Conduct

Foreign Corrupt Practices Act



What is the FCPA?

The Foreign Corrupt Practices Act (FCPA) is a U.S. law that prohibits companies and individuals from bribing foreign government officials to obtain or retain business. It also requires publicly traded companies to maintain accurate financial records and implement adequate internal controls to prevent corruption. The FCPA applies to conduct, both within the U.S. and abroad, and imposes severe penalties for violations, including fines and imprisonment.

We must also comply with the anti-corruption laws in countries where we conduct business.

Before offering a gift, hospitality, or other business courtesy to a foreign official, ask yourself these questions and always pre-coordinate with ITC or Legal:

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

Be Aware: **Facilitating payments (e.g., to expedite the customs processing of goods) are prohibited. Report any facilitating payment attempts or requests 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. Gift should not include items with inherent cash value or those that can be exchanged for cash.

SAIC FCPA and Anti-Corruption Instruction

BEFORE conducting ANY International Business, review SAIC instruction "Complying with the Foreign Corrupt Practices Act and Global Anti-Bribery Laws (SI-POL1-7)" on ISSAIC AND contact either ITC or the attorney supporting your business group.

Review SI-POL1-07 by clicking here

International Travel

Travel with approval

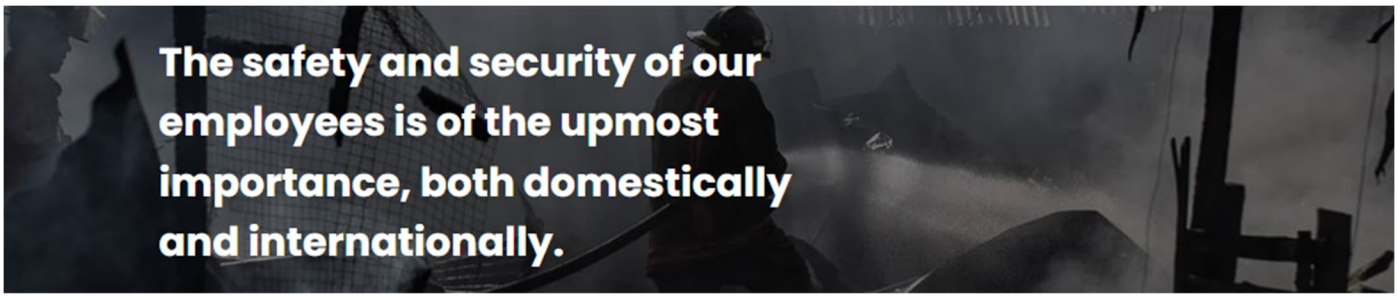
TC, Security, and Cybersecurity review all international travel requests (ITR) and provide guidance and oversight for corporate-wide compliance with U.S. export, import, and sanctions regulations. Before booking travel via Concur, you must complete an International Travel Request.

International Travel Request (ITRS)

- 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 at least 30 days prior to international travel
- Review SAIC's 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
- Any travel involving exports of technical data, defense services or hand carries of controlled hardware may require further ITC review.
- *The ITR can take up to 5 days to review and approve travel requests*

Be Aware: An International Travel Request (ITR) must be submitted prior to any travel outside the United States, including U.S. territories (Guam, Puerto Rico, etc.).

Crisis Management and Business Continuity



Visit the Crisis Guidancesite 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 Incident Response Plan
- Site-specific incident response plans to each SAIC facility

SAIC uses an Emergency Notification System that uses phone, text and email communications to connect with employees during an emergency. The mass notification system can send employees information, account for employees during an emergency, and compile the needs employees may have during an emergency.

Emergency Contact Information

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.

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

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

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

Background Investigations and Social Media

During the **security clearance process**, federal background investigators have the authority to look at **any public social media information** you have posted if they deem it necessary.

Continuous Evaluations/Continuous Vetting

In June 2022, the Office of the Undersecretary of Defense (OSD) announced the elimination of Periodic Reinvestigations (PRs), a significant shift affecting the contractor population cleared under the National Industrial Security Program, including DoD and branch service agencies, DIA, NGA, NSA, and DoS. In its place, an updated SF-86 must be submitted every 5 years from the date of the last background investigation or CV enrollment, whichever is most 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

The Director of National Intelligence mandates that all cleared employees be enrolled in a compliant Continuous Evaluation (CE) or Continuous Vetting (CV) Program.

CE - is an ongoing personnel investigative process which increases the timeliness of information reviewed between periodic reinvestigative cycles.

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
- 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.

You can access SEAD 3 and SEAD 4 below:

- SEAD 3
- SEAD 4

The 13 Adjudicative Guidelines are:

1. Allegiance to the United States
2. Financial Considerations
3. Foreign Influence
4. Foreign Preference
5. Sexual Behavior
6. Personal Conduct
7. Alcohol Consumption
8. Drug Involvement
9. Psychological Considerations
10. Criminal Conduct
11. Handling Protected Information
12. Outside Activities
13. Use of Information Technology Systems

The guidelines cover the following common situations:

- A change in personal status or significant life changes
- Financial considerations such as gains and/or losses
- Drug use (Federal law supersedes state law)
- Foreign travel and foreign contacts
- Litigation, arrests, court summons
- Traffic violations exceeding $300 in total fines
- Emotional or mental health consultation
- Computer misuse
- Mishandling of classified information
- Contact with the media
- Pre-Publication Review

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
- Alcohol and drug related treatment
- Apparent or suspected mental health issues that may impact the ability to protect classified or other secure information
- Personal Finance and Business Interests
- ALL personal foreign travel, 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
- Alcohol and drug related 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
- Any technical paper, book, magazine article, or newspaper article that you prepare for publication or for posting on the Internet, or lecture or speech that you prepare to give, must be cleared in advance if it contains information or knowledge you gained during your current or any previous job
- Testifying in court

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)

Outside Activities (For SAIC Personnel)

A personal conflict of interest arises when an employee's private interests conflict with his/her legal or moral responsibilities to SAIC or its customers. If you wish to participate in any of the below activities, you must complete a Conflict of Interest Agreement, which initiates the review and approval process. This agreement must be submitted and approved by the Ethics Office before you may participate in the proposed activity. You should discuss the proposed activity with your supervisor for initial guidance and permission to seek approval before beginning the review process. You may submit a request at any point during the year.

Activities that require a Conflict of Interest Agreement:

- Working for yourself or any organization, whether public or private, paid or unpaid, that is outside of your employment with SAIC
- Have a financial interest in a customer, competitor or supplier of SAIC
- Conducting research or instructing on defense or military matters
- Serving on a federal advisory or for-profit/non-profit board or committee
- Running for or accepting an appointment to public office
- Conflict with SAIC work schedule and/or Acceptable Use of SAIC Information and Assets instruction
- Working for or representing a foreign government or foreign owned business/organization
- Any activity that is substantially similar to one of the above-listed activities

An approved OAR must be renewed annually if the conflict of interest continues; the renewal must be submitted prior to the current OAR expiration date. If the facts supporting the original OAR change in any way, a new OAR must be submitted immediately.

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 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.

Mark Documents Correctly

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

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.

Secure Hand Carried Information

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

Handle the Media Appropriately

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

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.

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
- Misuse of Information Technology

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.

Refer below to see what type of damage unauthorized disclosure could cause:

- Confidential: Damange to National Security
- Secret: Serious Damage to National Security
- Top Secret: Exceptionally Grave Damage to National Security

Learn more about Classifiers below:

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 Classifier 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.

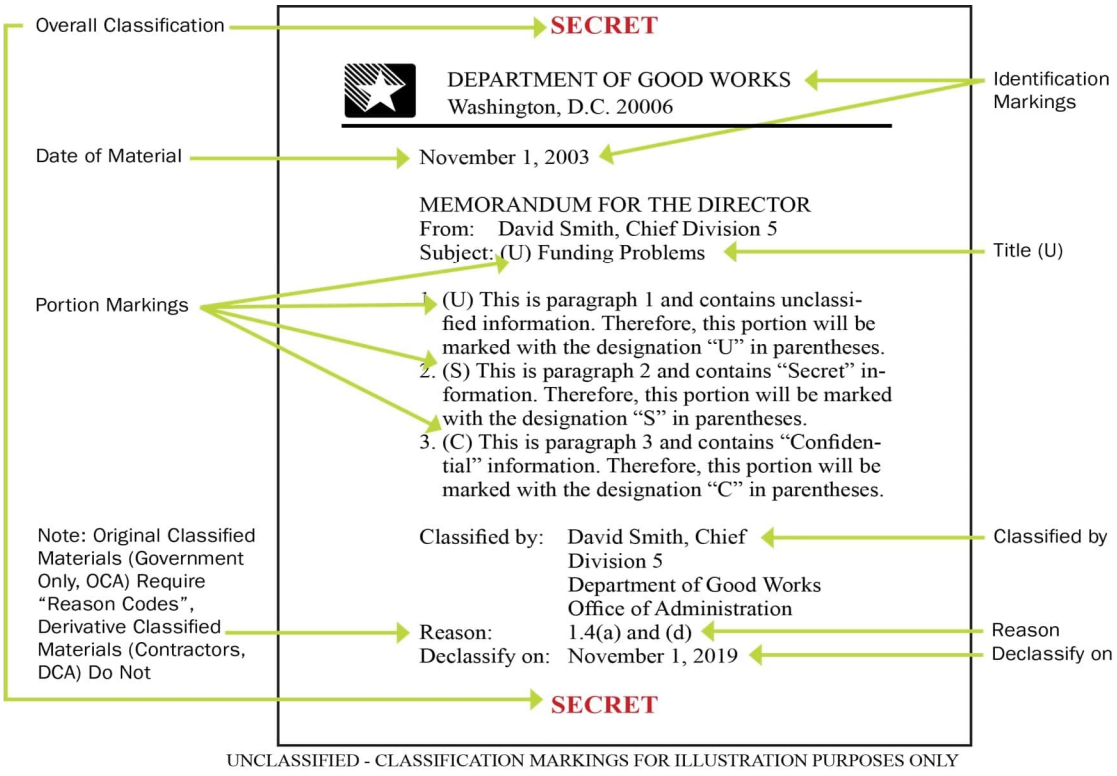
Never originally apply classification markings, downgrade classified information, guess or assume classification levels, or provide “subject matter expertise” or classification guidance to any source unless authorized by an OCA or classification guide.

Classification Marking

Classification portion markings and banner markings are 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:



UNCLASSIFIED - CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

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 Oversite 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

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

Safeguading 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

- Use Caution!!
- Compilation of unclassified facts could make the information classified.

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.

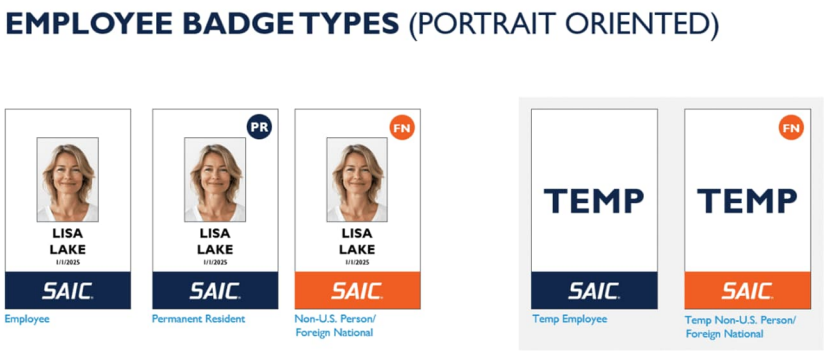
Security Badges

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.

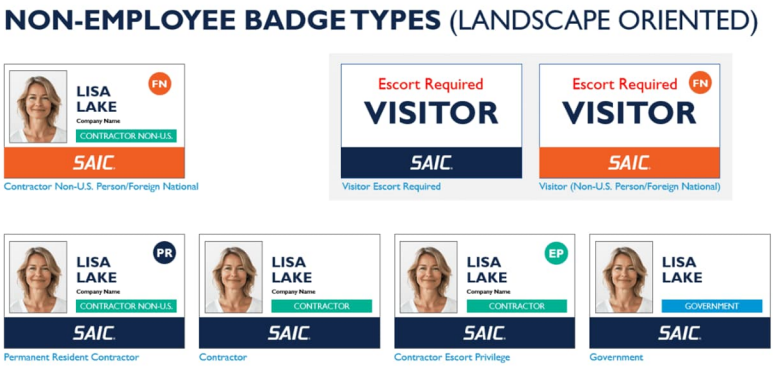
To protect SAIC employees and property, follow these simple rules:

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

SAIC employee badges are portrait oriented:



Non Employee Badges are landscape oriented:



Prohibited Items at SAIC

The following Items are prohibited at SAIC facilities (Please refer to SAIC Instruction SI-HR-21 - Prohibited Items for more information):

- 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.

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

Both Personally-owned and SAIC-issued Portable Electronic Devices (PPED) are 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:

1. Coordinate specifics with your local SAIC FSO/PSO as early as possible, but no later than 5 business days prior to the meeting
2. Ensure individuals in attendance have a Need-to-Know and clearances have been received.
3. Establish the security level of the meeting
4. 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.
5. Know the approvals in place for the conference room you are using
6. 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.

Counterintelligence and Operational Security

Recognizing Threats

Counterintelligence

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 Inisder Threats discussed earlier, external threats are more broad reaching and organized:

Foreign Intelligence Services (FIS)	Foreign & Domestic Industry Competitors	Criminal Activist & Terrorist Organizations
Can come from non-ally countries and our own ally countries.	Will commit industrial espionage to gain information to gain a competitive edge.	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.

1. Identify Critical Information: What do you want to protect and why? Is it unclassified, but sensitive? Will an adversary gain advantage by having the information?
2. Analyze the Threat: What does the adversary know? What is their intent? Where are they likely to gain the information?
3. Analyze the Vulnerabilities: Where are the weak spots? Are there any protections in place?
4. Assess the Risk: Is the risk great enough to take action? Is loss of sensitive data imminent? What's the cost?
5. Apply the Countermeasures: Begin with high risk vulnerabilities. Mitigate the risk factor with a plan and monitor the outcomes.

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:

Keep a Low Profile

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

Be Observant

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

Report Suspicous Activity

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

Do Not Share Sensitive Information

- Identify, control, and protect 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.

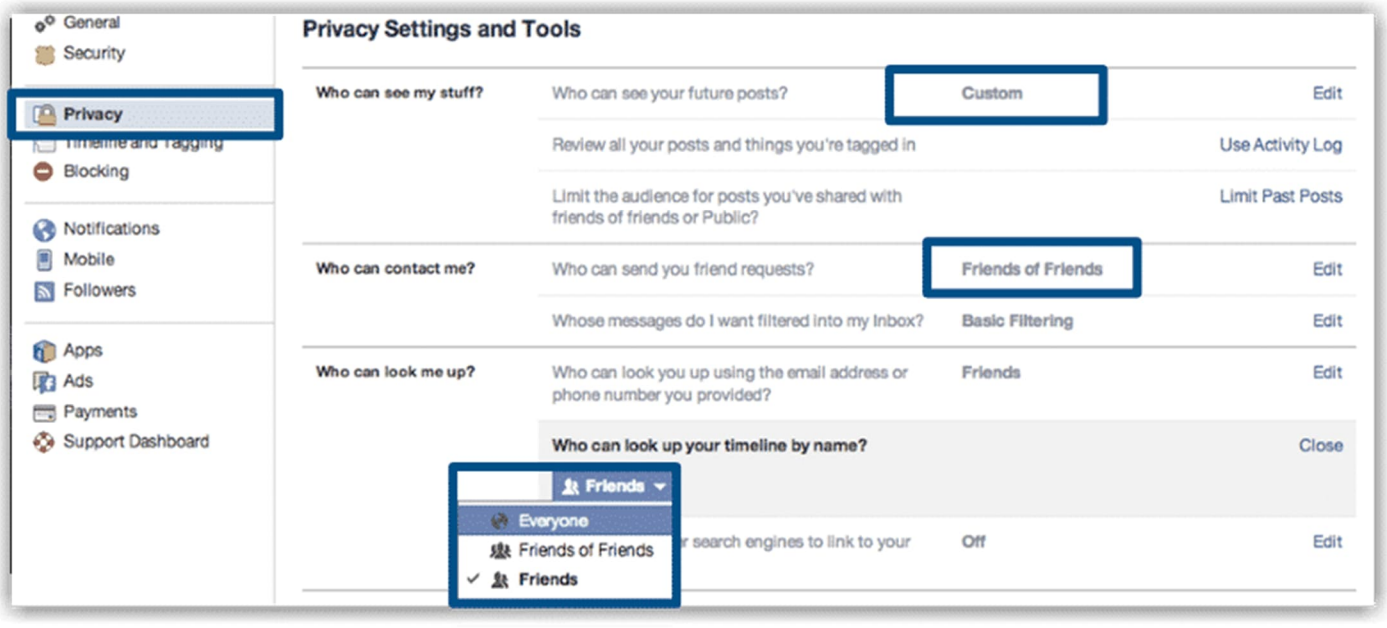
Although a variety of internet sites support SAIC business purposes, others are inappropriate to access using SAIC systems.

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.



Reporting Counterintelligence Threats

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

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!

Congratulations

You have completed the

2026 SAIC Annual Security Reindoctrination(ASR) Training

