ANNUAL SECURITY REFRESHER TRAINING

This annual refresher training is provided to you as a reminder of your obligations and responsibilities as a cleared individual.

INTRODUCTION

Upon completion of this module, you should be able to:

- Reaffirm your obligations that you agreed to when you received your security clearance or access.
- Describe types of government information, implement safeguards, and report data spillage.
- Be alert to and appropriately report potential threats by adversaries, insiders, and other harms.
- Carry out your responsibilities when escorting visitors.
- Understand your personal reporting responsibilities and obligations under the United States espionage and sabotage acts.

MEETING OUR SECURITY COMMITMENTS

Northrop Grumman is accredited to perform classified work. You have been granted a security clearance or access based on the company's requirements and customer's determination. Customers perform comprehensive security reviews to assess our performance of security obligations. Violations of our obligations could place the company and cleared individuals at risk of losing the eligibility to perform this type of work.

YOUR OBLIGATION – LEGAL AND BINDING

When receiving your clearance or access you confirmed by signing a non-disclosure agreement that you understand the consequences of violating your cleared obligations and agreed to:

- Accept a life-long obligation to protect classified information.
- Submit for pre-publication review any writing intended for public distribution.
- Protect classified and sensitive information
- Avoid unauthorized disclosure, retention, or negligent handling of sensitive government information and materials.

While there are a number of statutes mentioned in this agreement, violations of the statutes of Title 18 or Title 50 of the United States code can lead to prison sentences, fines, or both.

GRADUATED SCALE OF DISCIPLINARY ACTIONS

In addition to your previously discussed obligations there is also a graduated scale of discipline here at Northrop Grumman. This principle assigns appropriate administrative actions when a security violation occurs.

Northrop Grumman will work with Human Resources and use Company Principles and Operating Practices (PrOP) manual USHR 2-21, Employee Conduct and Discipline, graduated scale of disciplinary actions as a guide in determining appropriate administrative actions to assign to security violations.

Such discipline may include, but not limited to the following:

- A verbal warning
- A written warning
- A final written warning with or without unpaid suspension
- Discharge

Failure to follow established security procedures is viewed as a serious performance issue and shall be a factor to be considered in the performance review process. See CTM H200, United States Human Resources Manual.

PROHIBITED ITEMS

While at Northrop Grumman please be mindful of Prohibited items that are not allowed on property as well as those items that cannot be brought into secure areas. In addition to those listed here some other items such as cameras and recording devices are limited use and require prior approval.

Review Chapter 8 of CTMJ100 for complete details.

PROHIBITED ITEMS- All Sites

- Firearms, ammunition, projectile weapons, and incapacitating agents or devices, except when required by law enforcement, military, or authorized security personnel.
- Bladed, edged, or sharp tools or implements, except for company-approved and issued tools of the trade and personal folding pocket knives with a blade length of less than 2.5 inches.
- Club-like items and striking devices.
- Explosive and incendiary devices.
- Alcoholic beverages.
- Illegal drugs and other controlled substances, as defined by federal law, that are not legally authorized for the holder.

PROHIBITED ITEMS within DoD Storage Areas

- Computers (desktop or laptop)
- Cellphones, tablets, blackberry's, Televisions
- Cameras, video players
- Smart Watches
- MP3 Players
- Thumb Drives
- Remotely controlled medical devices*
- MP3 CDs
- Two-way devices (radios, walkie-talkies, pagers)
- Tape Recorders
- Headphone with Wireless, Bluetooth, Noise Cancelling/Microphone capabilities

**Note: Some medical devices such as hearing aids and insulin pumps may have Bluetooth capabilities.*

If you are unsure if a device is authorized, contact your local security office prior to entering a restricted area. In the event that you or another individual brings a prohibited item into a restricted area, remove the prohibited item from the area immediately, secure it, and then contact your local security office for reporting requirements.

TYPES OF GOVERNMENT INFORMATION

There are two categories of government information that you might handle in your work – unclassified and classified.

Unclassified government material is material that does not require a security clearance. However, it can still be very sensitive information and require special handling.

Types of unclassified include CUI, formerly FOUO.

Unclassified material that is co-mingled with classified material must be marked.

The statement of work provided with your tasking or the overall contract document will provide specific instructions on the handling of these types of materials. For further guidance, consult your program manager, supervisor, contracting officer or security representative.

CLASSIFIED GOVERNMENT INFORMATION

Classified government material requires the person handling or given knowledge of the information have the required clearance or access for that information and a need-to-know.

When classified material is generated, it carries one of the following designations:

- "Originally classified" is material classified by a government official or so designated in writing by the President of the United States.
- "Derivatively classified material" is any material subsequently derived by a source document(s) or from guidance provided by a Security Classification Guide or DD254 (a government directive form). As a cleared contractor employee creating classified materials, you are a derivative classifier.

You are responsible for reviewing the Security Classification Guides and directives associated with your program. Classification guides are available from your Security office. If you are unsure how to interpret the classification guide, consult your supervisor or manager. It is your responsibility to determine appropriate classification and proper marking.

If you come across information that you think is improperly or unnecessarily classified, contact your local Security team to discuss. You must continue to protect the information at the level identified in the Security Classification Guide, until a formal review is complete.

PROTECTING CLASSIFIED MATERIALS

Protection of classified information is critical to our national security. The purpose of properly classifying only what is required to be classified and only for the duration permitted is to promote the sharing of information when allowed:

- Always maintain direct control of classified information.
- Provide access to classified material only to those with appropriate clearance and with a need-to-know.
- Review your holdings annually.
- Never confirm, deny or comment on classified information; Understand that classified information reported in the press or available on the Internet is still classified.
- Conduct an end-of-the-day security check for yourself and your work area to ensure that:
  - Systems are shut down, locked and password protected.
  - Material is properly stored.
- Containers and areas are secured.

WORKING REMOTELY

For many, working remotely is now part of our daily routine. For some it is a necessity, others a nicety. But remote working introduces additional personnel security risks that do not occur while operating within our facilities.

Working remotely entails the transit and storage of information outside the secure corporate infrastructure, with an increased risk of interception. Home Wi-Fi networks are more vulnerable to hacking and are being actively targeted by cyber criminals looking for weaknesses. When mobile devices (laptops and mobiles) are used outside the office, there is a higher vulnerability to theft, loss and malicious attacks.

Here are some recommendations for staying secure while working remotely:

- Assess the physical security of your working area, especially where there is uncontrolled shared access. Make sure your screen cannot be seen by anyone passing by.
- Store proprietary documents and unencrypted media in places not readily observable or accessible to non-employees (e.g., in a briefcase or cabinet).
- Ensure your home Wi-Fi is set up securely, using a strong password and encryption. We recommend changing your security password every 90 days, at minimum.
- If you are not alone, hold conversations where you are less likely to be overheard and position your screen where it is less likely to be seen.
- Immediately connect to VPN when signing on to your company device.
- Turn off virtual assistants (i.e., Alexa, Google Echo) when conducting work related calls.
- Do not store your credentials or PIN with your devices. While 15 characters are required, we recommend using an 18-character password that is hard to figure out.
- Always lock your screens when leaving the general vicinity of your device.
- When your company device is not being used, power it down so it is inaccessible, keep it somewhere safe so it cannot be stolen or tampered with. Never leave it unattended in your car.
- Never use your personal email to conduct company business or email company information to your personal email or any non-Northrop Grumman account.
- Personal peripherals may be connected to your company device as long as the peripheral does not have non-volatile memory (e.g., headset, mouse, keyboard, monitor). Personal printers must be powered off after printing company information.
- If you need to print company information to your home printer, contact the IT Service Center for support.
- If you feel that there has been a compromise of any type of protected information, report it as soon as possible to the Cyber Security Operations Center (CSOC) or Security.

ESCORTING REQUIREMENTS

All employees who possess a DoD clearance or have special access to a restricted area are required to know their escorting requirements. In the event that you need to bring an uncleared visitor (one that does not possess a DoD clearance or is not SAP/SCI briefed) into a restricted space, please follow your escorting requirements. If you are unsure of an individual's clearance level or need-to-know, please contact your local security for verification prior to allowing entry to a restricted area. Do not bring a visitor into a restricted space without following the escorting steps outlined for your specific restricted area, which may include the following common steps:

- Keep the visitor within sight and in your control at all times.
- Only provide the visitor access to approved areas essential to the purpose of the visit.
- Coordinate with Security before taking the visitor into classified, closed, or restricted areas.

- Prevent the unauthorized exposure to company proprietary information. If disclosure is authorized, inform the visitor of the proprietary nature of the material.
- Ensure the visitor understands and does not violate restrictions on the use of personal devices or prohibitions of photography and recording on company premises.
- Ensure the visitor does not connect non-company devices to company networks or devices unless specific, prior Information Security approval has been obtained.
- Follow site Security requirements for the return of the visitor badge.
- Prior to entering the restricted space, notify everyone along your planned route that you are about to bring in an uncleared person. This will allow adequate time for the area to be sanitized of classified information and classified systems can be locked appropriately.
- Ensure the uncleared individual locks up all prohibited Bluetooth and/or wireless devices prior to entering, with the exception of any emergency personnel
- Bring the uncleared visitor into the space and announce "UNCLEARED IN THE AREA". Turn on the overhead warning light, if applicable.
- Sign the visitor log appropriately
- Escort the visitor along the pre-planned route with a hand-held flashing light, if available, and constantly announce "UNCLEARED WALKING THROUGH"
- Ensure areas are sanitized before allowing uncleared to pass to prevent inadvertent disclosures.
- When the work is complete, exit down the same path as you entered, continually notifying employees in your vicinity that the uncleared visitor is walking through
- As you exit the area, sign the visitor out of the log and turn off any warning light

If you need additional escorting training, please contact your local security office.

Escorting requires you to be within line-of-sight of the uncleared individual at all times. In the event that you need to leave the restricted area prior to the work being complete, please pass off escorting duties to another cleared employee or have the uncleared individual exit the area with you.

Failure to follow your escorting requirements could result in a possible compromise to classified information, resulting in a security infraction or violation. If you have any issues during escorting or believe there was a possible compromise of classified information, please contact your local security immediately.

NON-U.S. CITIZEN VISITS

Visits of non-U.S. citizens or Foreign Persons to company U.S. facilities must be coordinated in advance with Security and Export Control to ensure compliance with requirements and responsibilities associated with ITAR/EAR (International Traffic in Arms Regulation/Export Administration Regulations). Remember that Northrop Grumman employees representing entities located outside the U.S. may have the same requirements as other foreign visitors. The Northrop Grumman sponsor must process a Foreign Visitor Request through the Enterprise Export

Management System (EEMS). See CTM J100 *Company Security Manual* for all requirements, process, and definitions of non-U.S. citizen and Foreign Person. Some facilities may have more stringent, contractual security requirements.

If you are a host or an escort to a Foreign Person visitor, you have specific responsibilities detailed in CTMJ100.

- Corporate Form C-878 Acknowledgement of Escort Responsibilities

HOSTING CLASSIFIED MEETINGS

At the start of a classified meeting, set and announce the level of the meeting. Prior to beginning any classified discussion or disseminating any classified information, the meeting host is responsible to ensure:

- The location is secure and discussions cannot be overheard.
- Attendees have the appropriate clearance and access levels.
- Attendees have need-to-know.
- Electronic devices are removed or powered off, depending upon procedures.

Remember, never process classified information on an unclassified computer system. The meeting host can coordinate with Security if a classified computer is required.

Take actions immediately if you notice that someone has an electronic device or if you can hear conversations from another meeting room, indicating that your meeting conversations may also be overheard.

CODE BLUE – AWARENESS AND REPORTING

The company maintains the required high level of protection for classified information. We must all be aware of the potential for classified information being inappropriately introduced into an unauthorized information system(s). These are known as data spills.. Code Blue is the unclassified name established by Northrop Grumman to describe the occurrence and remediation process used when government classified information is introduced into unclassified Northrop Grumman information systems and/or media and portable devices within Northrop Grumman facilities.

Immediately report a suspected Code Blue to your Security point of contact. If you are not able to reach a Security point of contact, report the potential Code Blue directly to the Cyber Security Operations Center (CSOC) at 877-615-3535. When reporting a Code Blue, do not disclose possible classified information over unsecure channels.

Follow these instructions to prevent further proliferation:

- Do not delete or forward any information.

- Do not attempt any cleanup of the information on your own.
- Disconnect the computer, and do not use the affected system until you are told that it is safe to do so.

References:

- CTM J100 *Company Security Manual*
- Code Blue (sharepoint.us)

INSIDER THREAT

"Insider threat" is the term used for the potential harm posed by individuals who have direct access to company networks and information.

Insiders committing illegal acts and unauthorized disclosure can negatively affect national security and industry in many ways. These acts can result in:

- Loss of technological advantage
- Compromise of classified, export-controlled, or proprietary information
- Economic loss; and
- Even physical harm or loss of life.

These types of threats from trusted insiders are not new, the increasing numbers of those with access to data and the ease with which information can be transmitted or stored can make illegal access and compromise easier.

LOOK FOR AND REPORT INDICATORS OF POSSIBLE INSIDER THREAT

We must all be on the alert for behaviors that might be indicators of an insider threat. Knowing the safeguards that must be applied to handling company and customer information, report behaviors such as:

- Mishandling or misusing company or customer information
- Removing company or customer information from premises for unauthorized, personal, or unknown reasons
- Copying company or classified information unnecessarily
- Engaging in classified conversations without a need-to-know
- Establishing unauthorized means of access to company or customer information systems
- Seeking access to company proprietary, controlled sensitive, or classified information on subjects not related to job duties

Other behaviors that might indicate a possible insider threat include:

- Unreported foreign contacts or overseas travel
- Sudden reversal of financial situation or repayment of large debts or loans

If you observe any of these behaviors or suspicious behaviors by an individual, report the activity to your management, Security, or the MySecurity website.

While not all suspicious behaviors or circumstances represent a threat, each situation must be examined along with information from other sources to determine whether or not there is a risk. Observing even a single activity and not reporting it can increase the potential damage that can be done.

- case-study-henry-frese.pdf (cdse.edu)
- case-study-christopher-victor-grupe.pdf (cdse.edu)
- CTM J100 *Company Security Manual*
- Find Security contact information on your sector home webpage or on the Security Services page.
- Find other resources in the Counterintelligence & Insider Threat (sharepoint.us)section on the Enterprise Security Intranet (sharepoint.us)

THREAT LANDSCAPE

Our company and its employees are a prime target of many foreign intelligence collectors and government economic competitors attempting to gain military and economic advantages.

Adversary Method: Elicitation

Elicitation is the strategic use of conversation to subtly extract information about you, your work, or your colleagues. Foreign intelligence officers are trained in elicitation tactics.

The Internet and social networking sites make it easier to obtain information to create plausible cover stories. Unsuspectingly, a conversation or relationship that starts out purely social gradually provides information or part of a puzzle that the foreign operative can combine with other information.

Employees should always be aware of the possibility of elicitation attempts both at work and in casual settings. Be prepared by knowing what information you cannot share and be suspicious of those who seek that information. If you believe someone is attempting to elicit information, you can say you don’t know, refer them to the Internet, try and change the topic, or provide a vague answer.

Because elicitation is subtle and can be difficult to recognize, report any suspicious conversations to Security or the MySecurity website.

Attending a trade show or conference? Understand the limits of information you can provide. Report contacts if you experience insistent questions outside of the scope of what you have already provided or attempts at unnecessary ongoing contact.

Are you a subject matter expert? Report unsolicited requests for assistance; requests to review thesis papers, drafts publications, or research-related documents; or unsolicited invitations to attend international conferences.

Don't reply to unsolicited requests for information. Suspicious email can be reported to the Cyber Security Operations Center at CSOC@ngc.com. Report suspicious phone contacts to the MySecurity website.

Safeguards When Participating in External Conferences

If you are participating at a conference or meeting as a speaker, discussion panelist, or moderator where you are identified as a Northrop Grumman employee, follow Corporate Policy CPA6 *Employee and External Communications*, or your sector's Communication procedure for clearance of public speeches.

- Don't connect your laptop to conference-provided networks or connect to the company network using their computer kiosks.
- Beware of potential eavesdropping when having work-related conversations in-person or over the phone.
- Report unusual contact attempts or occurrences to Security.

Reference:

- Where to Report webpage
- Security Points of Contact webpage

Adversary Method: Recruitment

Recruitment is obtaining cooperation from someone to provide information.

Anyone with information or access to information could be a potential target. Safeguard your actions and words to avoid becoming an easy target.

You may not realize at first that you have been spotted for possible recruitment. In initial contacts the adversary will try to determine if you have information or access of value, or if you might have such information in the future.

If the adversary is interested, he or she will attempt to develop the relationship and devise a ruse to establish a logical basis for continuing contact. The adversary will continue to assess your willingness to provide information.

The adversary's goal is to establish a relationship of friendship and trust. It could start with requests such as professional advice or information about a co-worker. You might have a sense of obligation and not see any harm in complying. The adversary could then move the relationship along and step-up the information requests, for example, as a consultant.

Use caution if you feel you are being recruited.

- Listen carefully
- Be observant
- Remember as many details as possible
- Keep all options open by neither agreeing or refusing to cooperate
- Stay calm
- Be non-committal
- Ask for more time

Inform your Security Representative immediately if you have any suspicious conversations or suspect you are being recruited.

You are not being asked to avoid all foreign contacts. Your main defense against espionage is being aware of the signs of recruitment and elicitation, knowing not to respond to even seemingly casual questions for more information about the work that you do, and reporting all suspicious contacts to your Security office. Contacts can come in various forms, either in-person or online.

- Where to Report webpage
- Security Points of Contact webpage

REPORTING

Compliance with security requirements is an on-going part of your position. The purpose of reporting possible threats and compromises is to detect and mitigate any vulnerability to our country and its resources, which includes Northrop Grumman and our employees.

Immediate threats and security compromises should be reported directly to your local Security team. The MySecurity website can be used to report suspicious activity, including insider threat, and suspicious contacts. These reports will be sent to your site specific designee.

Northrop Grumman employees are encouraged to report within company channels prior to contacting the government defense hotline. However, if you are not satisfied with the results of your contact at the company level, you are encouraged to report to the DoD hotline. Comments and questions made during these contacts must be kept unclassified.

- Phone: 800-424-9098
- Government e-mail: hotline@dodig.osd.mil
- Web: http://www.dodig.mil/hotline

If your report deals with a special access program use that approved reporting method versus the process described here.

- CSOC (Cyber Security Operations Center): CSOC@ngc.com or 1-877-615-3535 monitored 24x7
- Ethics and Business Conduct for links to Business Conduct Officers and OpenLine

(OPERATIONS SECURITY) OPSEC PROCESS

Operations security is a method of protecting our information. Compilation of unclassified information could lead to an adversary's ability to collect, process, analyze, and misuse that information.

Operations security (OPSEC) is a process to identify critical information and protect it from adversaries by controlling and protecting generally unclassified information. The process has five components:

- Identifying the Critical Information
- Analyzing the Threat
- Analyzing the Vulnerabilities
- Assessing the Risk
- Initiating the Countermeasures

Consider OPSEC daily by identifying information that should be not posted to public websites or thrown out in the trash or recycle bins. Share only on a need-to-know basis and dispose appropriately.

For example, while our company contact information is not sensitive information, we would mark contact information for employees at an entire site as Northrop Grumman Proprietary Level I so that the information is not inadvertently released outside of the company.

Could this be valuable information to an adversary?

If yes, then don't post it on social media:

- Nobody's going to be at work tomorrow – the network's going to be out!
- I just saw the budget figures for Project X – you won't believe it!
- They still can't get this right – still not passing QA.

BADGING

Wearing badges while at Northrop Grumman is a physical security measure used for the safety of individuals and protection of company information.

Wear your company badge in plain view, above your waist, at all times on company premises, unless you are using your OneBadge for computer access. When using your OneBadge for computer access, remain physically present and in control of your badge.

In addition to access to facilities, our badges may also allow access to computer resources and other privileges. Protect your badge from loss, theft, damage, misuse, and counterfeiting. Your badge should only be used for company purposes. When entering any Northrop Grumman facility or secure area, do not tailgate! Everyone must present their own badge or PIN to the card reader to confirm valid access. Ensure the door closes behind you. See local security if you require access and your badge is not programmed. Remove your badge when not on company premises. Don't store your badge with your laptop. Report lost or stolen badges immediately to your management and Security so that certifications and privileges written to the chip and magnetic strip can be suspended to prevent misuse pending resolution.

In a facility or area with badge-controlled access, if you encounter an unbadged individual or an unaccompanied individual with a badge marked "Escort Required," you should escort the individual to the nearest manned Security access control point.

- CTMJ100 – Company Security Manual

Be Sure:

- Don't leave your badge on display in your car.
- Don't use your badge for identification not related to company business.
- Don't allow your badge to be photographed, scanned, or otherwise reproduced.

YOUR REPORTING REQUIREMENTS

As a cleared individual, you have a legal obligation to report certain events, not only about yourself but also your coworkers. For a more detailed list, review the Reporting Guidance website. To identify your Security POC, use Check Your Status on MySecurity.

Reportable events include:

- Loss, compromise or suspected compromise of classified information.
- Known or suspected security violations involving classified data.
- Changes in personal status —such as: name change, marriage, divorce, cohabitation, citizenship, or when an employee no longer has a requirement for a security clearance or access. See your local program security team for specific guidance for this category.
- Becoming a representative of a foreign interest— including work or material support for an adversary government, company, or individual.
- All business and personal travel outside the U.S.

You are also required to report information of an adverse nature. Adverse information includes:

- Arrest or detention by any law enforcement agency.
- Tickets and fines greater than $300.
- Unfavorable financial situations such as bankruptcy, garnishment of wages, and excessive indebtedness.

- Unexplained affluence, anything from outside your personal financial (401K, home equity) or income channels, such as a sudden wealthy lifestyle without an increase in salary like family monetary gifts, inheritance, or winnings.
- Uncontrolled use of substances (alcohol, prescription drugs, or illegal narcotics).
- Treatment and counseling for mental or emotional disorders— excluding grief, family or marital counseling and treatment related to adjusting from military service, unless medication has been prescribed.
- Other matters that could have an adverse impact on your ability to safeguard classified or proprietary material.

Report events and adverse information to your Security Representative. This information will be held in the strictest confidence following company and U.S. government policy. If you are not sure if information is reportable, check with your Security Representative.

DOD

This portion of the security refresher module covers DoD specific information.

CLASSIFICATION LEVELS

There are three distinct levels of classification within the Department of Defense (DoD) system:

- Confidential
  - Confidential is information, that when compromised could cause damage to our national security.
- Secret
  - Secret is information, that when compromised could result in grave damage to our national security.
- Top Secret
  - Top Secret is information, that when compromised could result in exceptionally grave damage to our national security.

To access any of these three types of information you must have a clearance at that level or higher and a valid need-to-know.

DERIVATIVE CLASSIFIER

As a cleared contractor employee, if you create classified materials as a part of your job responsibilities either by incorporating, paraphrasing, restating or compiling information that is already classified. You are considered a derivative classifier.

To comply with government regulations, a derivative classifier must take training every two years to continue to create classified material or to have access to a classified computer system for DoD. are DoD

Derivative classifiers must use only authorized sources of classification guidance to derivatively classify information. There are only two authorized sources for derivative classification. SCGs are the primary source for derivative classification. A second authorized source for derivative classification is an existing, properly marked source document from which information is extracted, paraphrased, restated, and/or generated in a new form for inclusion in another document.

The only lawful reason to classify information is to protect national security. And that information must be declassified as soon as it no longer qualifies for classification, at the direction of an OCA. Information must not be classified, continue to be maintained as classified, or fail to be declassified for any other reason. Information is prohibited from being classified to conceal violations of law, inefficiency or administrative error, to prevent embarrassment to a person, organization, or agency, to restrain competition, or to prevent or delay the release of information that does not require protection in the interests of national security. In addition, basic scientific research and its results cannot be classified unless that information is clearly related to national security

SPECIALS

As a part of maintaining your additional accesses the following information is provided.

ACCESSES

You have access to Special Access Program, known as SAP or Sensitive Compartmented Information, or SCI. This information requires additional levels of protection.

OVERSIGHT AND GOVERNANCE OF SAP/SCI PROGRAMS

Oversight and Governance of SAP and SCI programs is executed by Congressional Defense committees in accordance with the policies and manuals:

Congressional Defense Committees execute all facets of oversight:

- Provided with advance notice of program
- Given detailed justification
- Gets estimate of total program cost
- Told of similar programs/technologies
- Once approved, monitor closely

SAP and SCI Security is governed by various policies and manuals:

- EO 12333
- EO 13526
- EO 12526
- All ICD policies
- DoD 5220.22-M NISPOM
- DoDM 5200.01 Vol 1-4 Information Security Manuals
- DoDM 5205.07 Special Access Program Security Manual
- Risk Management Framework (RMF) via Joint SAP Implementation Guide (JSIG)
- Program Specific:
    - DD 254s
    - Security Classification Guides (SCG)
- Company PrOP/Local standard operating procedures
- Other guidance as provided by your security officer

ACKNOWLEDGED, UNACKNOWLEDGED

There are three types of SAP programs; acknowledged, un-acknowledged and unacknowledged/waived

Acknowledged programs are programs that may be openly recognized or known. However, specifics are classified within that SAP. An acknowledged SAP is one that is acknowledged to exist and whose purpose is identified - such as the B2 or the F-117 aircraft programs, but the details, technologies, materials and techniques of the program are classified as dictated by government.

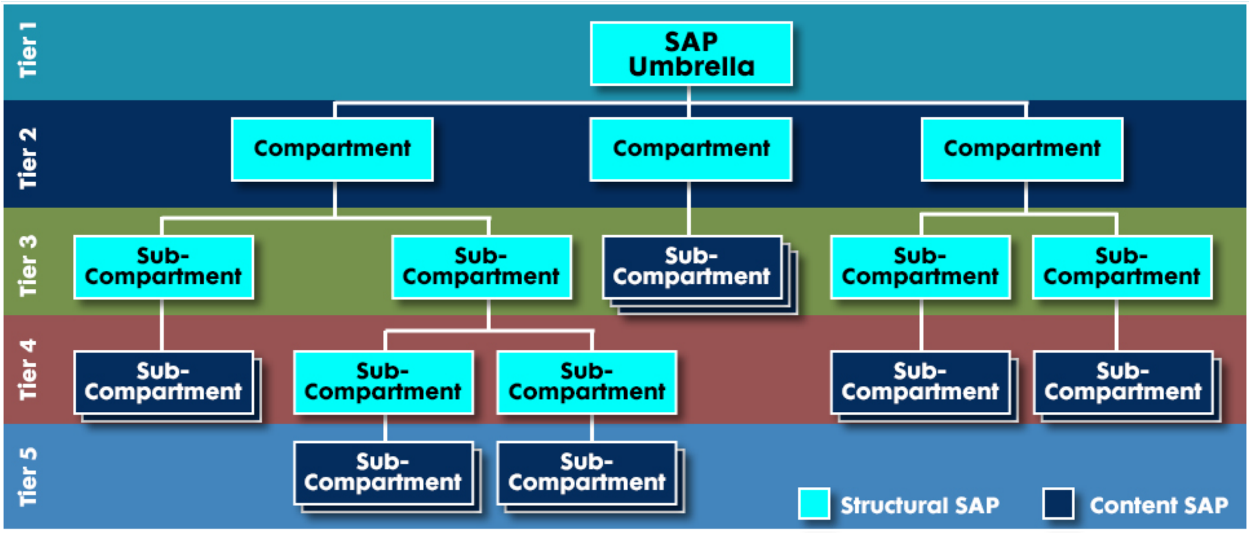
Unacknowledged programs are programs whose existence are not known or recognized and are protected as special access. The details, technologies, materials and techniques of the programs are classified as dictated by the government. Program funding is often unacknowledged, classified, or not directly linked to the program. In unacknowledged programs, even the existence of a relationship between Northrop Grumman and the customer is classified information and should be protected as classified, meaning the fact that you or the company is working with this customer should not be discussed in unclassified channels.

Unacknowledged/Waived is a SAP that has been waived by the secretary of defense for applicable reporting following a determination of adverse effect to National Security.

CATEGORIES OF SPECIAL ACCESS PROGRAMS

The DoD has replaced the legacy Special Access Program (SAP) hierarchy with a SAP architecture that organizes DoD SAPs in a manner that facilitates more efficient and effective oversight and governance. The SAP architecture is organized into a maximum of five tiers, comprised of SAP umbrellas, compartments, and sub-compartments. Each umbrella is designated as either “Joint Force Integration” or “Strategic Enabler”. The terms “content” and “structural” describe the role a SAP has within the architecture. The SAP may be content or structural but not both.

- Content SAPs protect Critical Program Information (CPI) associated with specific capabilities or information. Content SAPs are the lowest possible tier in the architecture.
- Structural SAPs organize and group content SAPs that protect similar capabilities of information. Structural SAPs are intended to have other SAPs subordinate to them in the architecture.



SECURITY CLASSIFICATION GUIDES AND CRITICAL PROGRAM INFORMATION

Security Classification Guides or SCGs, are a collection of precise, comprehensive guidance about a specific program, system, operation, or weapon system telling what elements of information are classified. For each element of information, the SCG includes its classification level, the reasons for that classification, and when the information can be downgraded or declassified.

Critical Program Information (CPI), in an acquisition program, may be classified information or controlled unclassified information (CUI) about technologies, processes, applications, or end items that if disclosed or compromised, would:

- Degrade system combat effectiveness
- Compromise the program or system capabilities
- Shorten the expected combat life of the system
- Significantly alter program direction, or
- Require additional research, development, test, and evaluation resources to counter the impact of the compromise

CPI includes, but is not limited to, CPI inherited from another program and CPI identified in pre-system acquisition activities or as a result of non-traditional acquisition techniques.

CPI is unique to every program and can be found in the Security Classification Guide (SCG). All program briefed personnel are required to be familiar with the SCG and CPI.

RELATIONSHIP OF SAP ELIGIBILITY TO SECURITY CLEARANCE

A DoD Clearance is the foundation of a person's ability to access classified information. For Special Access Programs (SAPs), an employee requires both a DoD Security Clearance as well as specific program access approval gained through the SAP Nomination Process (SAPNP).

- Minimum of a final Secret clearance is required to obtain SAP access.
- Interim TS clearance may be used to obtain Secret access to a SAP program.

CONTINUOUS VETTING/CONTINUOUS EVALUATION

The Continuous Vetting (CV) and Continuous Evaluation (CE) Program allows the government to defer a Periodic Reinvestigation (PR) for a specific person to a later date. When enrolled prior to when a PR is due, the CV or CE enrollment date will act like a new investigation date on PSQs and templates.

PRE-SCREENING QUESTIONNAIRE (PSQ)

Annually, SAP accessed personnel are required to complete an updated pre-screening questionnaire (PSQ) and associated forms based on the last completed investigation date or continuous evaluation enrollment date.

Additional forms or templates include five sections related to:

- Foreign Affection
- Foreign Association
- Foreign Travel
- Personal Conduct
- Financial Considerations

You are only required to complete the associated templates for any "Yes" responses to provide clarifying details.

For SCI, please contact your CSSO for additional reporting forms.

PROHIBITIED ITEMS WITHIN SAPF/SCIF

Be mindful of Prohibited items that are not allowed within SAPFs and SCIFs.

- Cellular phones (government-issued, corporate-issued, or personally owned; smart or classic "dumb" phones)
- Two-way devices (radios, walkie-talkies, pagers)

- Smart watches, smart shoes, and fitness devices with camera, microphone, Wi-Fi, cellular, or user accessible storage
- Laptops/tablets (government-issued) with built-in microphones or cameras unless physically mitigated (BIOS/UEFI/operating system settings are not sufficient)
- Corporate or personally owned laptops/tablets, and personally owned desktops
- Personally owned desk phones or desk phone headset devices.
- Unclassified webcams and video teleconference (VTC) units (e.g., DX80)
- Unclassified headsets with microphones, unless they are wired and push to talk (push to mute is not acceptable).
- Headphones with wireless, Bluetooth, or noise cancelling/microphone capabilities
- Desk phones that are not approved by the NTSWG (National Telecommunications Security Working Group). Headsets attached to NTSWG -approved desk phones must be wired.
- Voice-activated assistant devices (e.g., Alexa) and smart televisions
- Personally owned cameras, video, or MP3 players
- Removable media including but not limited to personally owned CDs, DVDs, thumb drives, and tape recorders
- Bluetooth or Wi-Fi enabled medical devices*
- *Note: All medical devices such as hearing aids and insulin pumps must be approved by the cognizant SSO, Program Security Officer (PSO), or Accrediting Official (AO) prior to entry to a SAPF/SCIF. Please contact your local program security representative to initiate the waiver request.
- Any other Wi-Fi capable device
- Any other current or future restricted device, as defined above or by specific SAPF/SCIF.

If you are unsure if a device is authorized, contact your local security office prior to entering a restricted area. In the event that you or another individual brings a prohibited item into a restricted area, remove the prohibited item from the area immediately, secure it, and then contact your local security office at your earliest convenience for reporting requirements.

ADDITIONAL REPORTING REQUIREMENTS

Additional reporting requirements not covered earlier in the training include:

- Employees briefed on Sensitive Compartmented Information (SCI) programs, Special Access Programs (SAP), and/or carrying company equipment/data must report all foreign travel, both business and personal. Reporting should be provided at least 30 days in advance (14 days in advance for official travel – travel fully funded by government or directly charged back a government contract) or as soon as the traveler becomes aware of the travel, and should be accomplished via ITRIP or the MySecurity website. Additional justification will be required for failure to report travel in advance.
- Continuous contact with foreign relatives and associations must be reported via the MySecurity website. This includes Facebook, LinkedIn, or other social network sites and classmates.

- Any contact with personnel from foreign official establishments, such as diplomatic services, law enforcement, military, etc.
- Any foreign financial interests or assets such as a vacation property, bank accounts, etc.
- Attendance at seminars or conventions where foreign representatives will be present.
- Legal involvements including subpoenas, witness involvement, or civil cases. Jury duty does not have to be reported.
- Tickets and fines greater than the program specified amount or $300.
- The desire to discontinue work on a special program.
- Questions from non-SAP briefed individuals about price, type, quantity, etc. of classified programs.

All of these should be immediately reported to your Security Representative.

Employees possessing SCI and/or SAP accesses are responsible to understand and comply with the reporting requirements for Foreign Travel, Post Foreign Travel and Foreign Contacts, consistent with the requirements of the U.S. Government sponsor of the individual employee's security clearance or accesses. Since some SAP and SCI Customers levy additional reporting requirements, employees briefed SAP and/or SCI must consult directly with their special program security representative to seek feedback and assistance in coordinating these requests with appropriate customer security. Refer to CTM J100 *Company Security* for complete details.

POLYGRAPHS

All employees who are submitted for and/or briefed SCI are subject to a government conducted polygraph exam. Personnel having access to DoD SAPs may be subject to a random polygraph exam. Depending on the government agency your typical examination consists of either counterintelligence or a full-scope polygraph, and on rare occasions you may subjected to a Issue-Based polygraph.

CI-scope polygraph: A screening polygraph examination that uses relevant questions limited to prescribed CI issues.

Issue-Based polygraph: Issue-based polygraph examinations is an examination that is predicated on an allegation or a specific issue under investigation.

Refusal to participate in a polygraph could have an immediate effect on your ability to hold a restricted access.

SAPF (SPECIAL ACCESS PROGRAM FACILITY) / SCIF (SENSITIVE COMPARTMENTED INFORMATION FACILITY) OPERATING ENVIRONMENT

Below are individuals responsible for the management and operation of the special access program:

Management	Roles and Responsibilities
Program Security Manager (PSM)	The PSM is responsible for assigning and managing a CSSO for each of the programs under their purview. The PSM will assist with escalation of issues to their program management counterparts and others as necessary.
Program Security Officer (PSO)	The PSO is appointed by the government customer SAPCO (Special Access Program Central Office) and is responsible for the program security management and execution of all security policies and requirements for a specific program, compartment, sub-compartment, or project. The PSO provides oversight and direction to the contractor SAP/special security officers (CSSOs) supporting their effort.
Contractor SAP/Special Security Officer (CSSO)	The CSSO is appointed by the Contractor Activity Manager (CAM) and is responsible for the overall Security cognizance of their Program and has the authority to appoint a designee when unavailable to perform their duties. The CSSO coordinates with the customer PSO and the Government Activity Manager (GAM) and CAM to create a secure environment and facilitate the successful development and execution of the SAP/SCI program at each organization or location where SAP/SCI information is stored, accessed or SAP/SCI-accessed personnel are assigned. The CSSO is responsible for security management and operations within their assigned activity.
Information System Security Manager (ISSM)	The ISSM serves as a principal advisor on all matters, technical and otherwise, involving the security of information systems under his/her purview. The ISSM is appointed in writing and approved by the PSO. When circumstances warrant, a single individual may fill both the ISSM and the ISSO roles.
Information System Security Officer (ISSO)	An ISSO is an individual responsible for ensuring the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the ISSM. The ISSO shall be appointed in writing and approved by the PSO. In close coordination with the ISSM and ISO, the ISSO plays an active role in monitoring a system and its environment of operation to include developing and updating the SSP, managing and controlling changes to the system, and assessing the security impact of those changes.
Briefed Personnel Responsibilities	All SAP/SCI-accessed personnel are responsible for adhering to all policies and procedures set forth by governing documentation whether Government or NG issued.
Custodian (Open/Close)	The individual that opens a facility for the day is responsible for closing the facility that day or handing off responsibilities to another individual that has been given open/close privileges for that facility.

SAP AND SCI SPECIFICS: RESUME

SAP and SCI specifics regarding your resume:

- Do not use digraphs, trigraphs, code words or platform names.

- You may state your DoD clearance, such as, Secret or Top Secret, and the type of investigation, such as Tier 3/Tier 5, along with the date.
- Never identify the program on which you work.

Be cautious when entering data onto your resume or performance appraisal about your specific job duties; use diligence to ensure the integrity of the program. Contact your local security team to review any resumes, appraisals, and performance reviews. Note, some customers may require you to submit your resume for approval prior to use.

COMMUNICATIONS SECURITY (COMSEC)

Classified conversations should only be discussed through secure channels. Check with the programs specific location to determine appropriate means for classified discussions. Ensure that:

- You completed your security department's security briefings.
- Do not discuss classified or program sensitive information on an unsecure telephone or in the vicinity of someone using an unsecure telephone.
- Do not talk around classified or sensitive information. All discussions should be on a Classified VoIP, STE, or vIPer phone at the appropriate security level of your discussion. You know who is on the other end before discussing classified information.
- Secure Phones may not be moved without prior approval by your Security Representative.

VISIT MANAGEMENT

Outgoing visits should be reported to your local Program Security team at least three days in advance.

Contact your local Security Representative with the following information:

- From location
- To location
- Start date of visit
- End date of visit
- Estimated arrival time on 1st day
- Subject of meeting
- Host POC/Phone number
- Names/driver license

Reminder: if you are visiting a covert location (i.e. Customer or Supplier sites), do not wear or bring any company identifying attire (i.e. clothing, hats, lanyards, etc.). When you are signing as a visitor follow local visitor procedures.

Incoming visits require the visitors' local program security team to send a visit certification in advance of the visit directly to the receiving program security team.

COMMON VS. DIFFERING ACCESS LEVELS

Do not assume that the person you meet has the same level of clearance or SAP/SCI level. Individuals may not be indoctrinated to the SAP and/or SCI accesses you possess, or they may have a lower classification level of the same program.

Classified information should never be shared unless:

- You have a need-to-know
- Security clearance
- SAP and/or SCI accesses have been verified through the CSSO.

Third Party introductions are allowed if the individual receiving the introduction is comfortable in accepting it.

- A third-party introduction is defined when an individual introduces one person to another for the first time. In this sense, the individual making the introductions also adds in the SAPs/SCIs the individuals being introduced are accessed to. *For example, "Harry this is Sally and she is briefed to the ABC and 123 programs. Sally this is Harry and he is briefed to the same two programs you are briefed into."*

Contact your local CSSO when there is doubt regarding the validity of a person's clearance or SAP/SCI accesses. It is better to err on the side of caution than to create a security incident and become another statistic.

SAFEGUARDING CLASSIFIED MATERIAL

Material must be properly stored at all times when not under direct control of an authorized person. When not in direct control, classified material must either be destroyed, locked in an approved container, or passed to another cleared employee to control. Any classified material left unattended will result in a security infraction or violation, due to a possible compromise to classified information. Please notify security immediately if you find classified material left unattended.

During an emergency, program accessed personnel shall take every possible measure to secure and protect classified information. Program accessed personnel are not expected to carry out protection and security actions at risk to their own safety or the safety of others.

Emergency Response Personnel (ERP) will not be prevented from entering this facility or any SAP/SCI area during or after hours for an emergency situation. Inadvertent Disclosure Statements will be prepared for each ERP who enter a SAPF/SCIF and may have been exposed to classified material or information. If no viewing or exposure to classified information, then an Inadvertent Disclosure Statement will not be executed.

During emergency evacuations secure material in approved containers. If you are unable to do so, notify the evacuation warden as you exit the area. Handling of combinations to classified storage containers are classified at the same level as the storage authority. You must protect and mark them accordingly when written. Combinations must be changed:

- When first installed or used.
- When there is possible compromise.
- When an individual who has the combination no longer requires access unless other sufficient controls exist to prevent that individual's access to the lock.
- When the container, vault, or secure room door is taken out-of-service or is no longer used to store classified information.
- At other designated times as defined by the security representative.

Remember to notify security before moving a classified container.

Additional information specific to the opening and closing of a SAPF/SCIF can be found in the location standard operating procedure.

SECURITY CLASSIFICATION MARKINGS

Security markings must be applied as a document is prepared and all documents and media must be marked appropriately. It is the generator's responsibility to classify program material in accordance with the applicable Security Classification Guide (SCG). Security markings include:

- Header/Footer on every page reflecting the highest classification of the document or the page
- Classification Authority Block
- Destruction Notices
- Portion Marking

The Classification Authority Block also known as the Classified by box, applies to cover page only is not applied to Unclassified, U//FOUO, CUI or U//HVSACO documents.

- Classified By indicates who is classifying the document including name and position
- Declassify Date is December 31st +50 years or the date of the declassify date from the source document
- Current Files Series Exemptions (FSE) date is 20150306

Portion Marking is required for all documents classified higher than unclassified and be placed at every element of the document including subjects, titles, graphics, tables, charts, subparagraphs, bullets, etc. Images, graphs and tables are portion marked in the lower right hand corner.

- Remember when portion marking attachments – you are portion marking the title of the document not the content of the document.

Any questions regarding marking material should be directed to your local program security team.

ADDITIONAL PROTECTION LEVEL: U//HVSACO

Unclassified Handle Via Special Access Channels Only or U//HVSACO is a protection level unique to SAP programs for unclassified information that must be limited to persons briefed into a Special Access Program with appropriate Need to Know and must be retained with SAP approved channels such as accredited SAP Facilities (SAPF) and approved information systems.

Information may only be designated with the “HVSACO” handling instruction by an OCA, as codified in the SAP Enterprise or an umbrella SCG.HVSACO documents require classification markings including banner and portion markings

HVSACO may be left unattended when a coversheet is placed on the front and back in areas authorized by the customer - contact your local Security team to see if your areas are approved for open storage of HVSACO material However, the best security practice is to store it in a locked desk drawer or safe.

CLASSIFIED MATERIAL COURIERING

All employees accessed to a SAP/SCI have the ability to courier classified material. If you need to transport classified material across your site or off-site, please contact your security office to receive the required training and approval. It is your requirement to know and follow all courier responsibilities. If you are travelling off-site, please contact your security office to receive an approved courier letter.

Be mindful that transporting items that require Two-Person Integrity, such as Top Secret material or writable media, requires two briefed persons to conduct the movement together. If you have any issues or concerns during your couriering, please report to your security office immediately.

DISPOSAL AND DESTRUCTION

All classified papers identified for destruction must be shredded using a PSO approved shredder. You should review your classified holding at least once a month and destroy any classified material that is no longer needed.

Other unclassified material generated inside the SAPF/SCIF may also be shredded such as:

- Yellow Sticky Notes
- Header pages from the classified printer
- Notes
- Calendars

CDs, DVDs, and any other media or irregular item must be brought to security for destruction

Note: Top Secret material is accountable material that must be tracked. The destruction of Top Secret material requires two SAP/SCI briefed personnel to perform the action at the direction of the SAP/SCI Accountability Officer and document completion on a destruction certificate. Only Security Professionals typically perform this action.

Please contact your local security team or review your local SOP for guidance.

SAFEGUARDING, STORAGE, PROCESSING AND HANDLING RESPONSIBILITIES

You are accountable for your actions while using any SAP/SCI information system. You affirm this responsibility and consent to monitoring every time you log on to the information system.

Program computers are for official SAP/SCI business purposes only. Computer activity is audited routinely for the following activities:

- Date and Time of your activities
- Activities involved
- System Performing the activities
- Resources involved

Remember to always lock your workstation when away from your desk and log off at the end of day. Do not let anyone else use your network account Do not write your password down.

INFORMATION SYSTEMS ROLE-BASED SECURITY TRAINING

The following shows the various roles and privileges of users within an Information System:

GENERAL User

- Are not allowed to create electronic media inside the SAPF/SCIF.
- If media is found (DVDs, CDs, thumb drives, etc.), bring them to your Program Security Officer.

PRIVILEDGED User

- Privileged Users are authorized by Program Security and IPT Management.
- All media must be labeled to indicate its classification level and other required markings.

DATA TRANSFER AGENT

- Data Transfer Agents (DTAs) are Security Professionals authorized to transfer information from low-to-high and high-to-low based on customer approved procedures.

TECHNOLOGY PROTECTION

Configuration Management:

- Computer hardware and software can only be installed by appointed personnel.
- Hardware movement within the SAPF/SCIF must be completed by appointed personnel and/or security (Classified and Unclassified).
- A minimum of one meter separation must be maintained between classified and unclassified IS and electronic equipment.
- All hardware entering or exiting the SAPF/SCIF requires prior approval by the program's Information Assurance Representative and the IS Custodian's completion of a "Hardware Entrance/Exit Form."

SECURITY INCIDENT TRENDS AND COMMON MISTAKES

A review of recent security incidents (past 18 months) revealed an overwhelming majority of infractions involved prohibited items entering restricted/program areas for durations of time spanning from seconds to hours. Prohibited items commonly involved in recent incidents include, but were not limited to:

- Cellphones (business/personal)
- AirPods or similar
- Apple Watches or similar
- AirTags or similar
- Oura Rings or similar
- USB devices

Another common incident trend included the failure to secure program areas when they are no longer occupied at the end of a session or meeting. Program areas must be secured when no longer occupied. It is imperative to validate whether you are the last person in a space prior to leaving and also ensuring that one or more of the remaining occupants can lock and alarm the area.

Regarding data spills, the most common occurrence was instances of Unclassified//Handle Via Special Access Channels Only (U//HVSACO) information being communicated outside of Special Access Program (SAP) channels. These channels include secure, approved SAP communications systems, SAPFs, and PSO-approved SAP storage areas.

SECURITY INSPECTION COMMON TRENDS

The self-review and external customer audits are critical to the continuing protection and success of SAP/SCI programs. Common trends during SAP/SCI customer inspections and other self-reviews often include:

- Not properly safeguarding classified information.
- Compilation of unclassified information resulting in inadvertent disclosure of classified information.
- Transmission of classified and sensitive information over unsecure program channel.
- Not properly marking classified documents and/or equipment (IT assets and/or program hardware).
- Lack of Security Education and Awareness.
- Weekly Information Systems (IS) audits not conducted.
- Insufficient entry/exit inspections.
- Inconsistent media control (site-wide).
- Incomplete records in USG systems of record (e.g., DISS, JADE, SC).

FRAUD, WASTE, ABUSE AND CORRUPTION (FWAC)

Employees are required to report fraud, waste, abuse and corruption.

Examples of fraud, waste, abuse or corruption:

- Intentional misuse of government assets
- Knowingly making false claims or statements to the government
- Acceptance of gratuities not permitted by law or regulation
- Falsification of test results
- Intentional falsification of time charging
- Purposefully charging government contract costs improperly
- Misuse of company resources (i.e. computers, Internet)

Refer to your specific program security classification guide for the telephone number to report fraud, waste, abuse or corruption. Your program specified FWAC reporting telephone number is displayed in each program area.

Information reported is maintained in confidence with no unauthorized release of your identity.

CONTACT INFORMATION

If you have questions or comments, contact your local Security Representative.

If you cannot view this video on the Learning Exchange (LX), email the ESSS Training Group at ESSS_DoDTraining@ngc.com stating you have completed the Security Refresher DoD / Specials training. In your e mail include:

- Your legal first and last name
- Your MyID
- Title of training completed: **Security Refresher DoD / Specials**