

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 restricted 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. Please contact your local program security representative prior to entering any SAPF so a waiver can be coordinated with the specific customer.*

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.

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.

PROTECTING CLASSIFIED MATERIALS

Protection of classified information is critical to our national security.

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, retain for only as long as needed, and properly disposition them when no longer needed.

Understand that classified information reported in the press or available on the Internet is still classified. Never confirm, deny, or comment on classified information.

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.

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 8 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 has no volatile memory (i.e., headset, mouse, keyboard, monitor, etc.). 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:

- 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. However, 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. Northrop Grumman refers to a data spill as “Code Blue.”

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.

Cyberspace enables social engineering attacks with readily available information about businesses and people.

For example, spear phishing attacks use social engineering to trick an individual into providing information or clicking on a link or attachment containing malicious software that can provide unauthorized network access, ex-filtrate information, or do other harm.

Report spear phishing and suspicious activity, for example anomalous computer behavior to the CSOC at CSOC@ngc.com or 1- 877-615-3535.

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. Unsurprisingly, 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. If you are a derivative classifier, this training will be assigned to you.

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 training.
In your e mail include:

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