INITIAL DOD TRAINING - REINSTATEMENTS

Congratulations! The results of your Background Investigation (BI) have confirmed that you are eligible for access to classified material.

An initial security briefing is required before being granted access to classified information. This briefing covers the basic security requirements of obtaining and maintaining a DoD security clearance.

Your specific clearance level is contained within the e-mail that you received. In addition, your local Site Security Representative was copied on the same e-mail. For site specific security requirements check with your local Security representative.

BOUND BY LAW

As a part of receiving your security clearance, you will be signing the Standard Form 312, a U.S. government Non-Disclosure Agreement. Even though you may not have signed the agreement yet, you are bound as part of the clearance process to the below requirements.

This document is a legally binding agreement between you and the United States Government. While there are a number of statutes mentioned in this agreement, there are two titles that provide specific punishments for violations. Disobeying any of the statutes of Title 18 or Title 50 can lead to:

- Prison sentences,
- fines,
- or, both.

You are encouraged to familiarize yourself with the statutes of these titles by visiting the sites shown.

Title 18: http://uscode.house.gov/browse/prelim@title18&edition=prelim

Title 50: http://uscode.house.gov/browse/prelim@title50/chapter23&edition=prelim

YOUR OBLIGATION

By signing the Standard Form 312, you are agreeing to accept a lifelong obligation and acknowledging your conformance with NISPOM/32 CFR 117 and other government regulations relative to your clearance and access to classified. In addition, you agree to:

- Protect classified and sensitive information
- Submit any writing for pre-publication review

- Avoid unauthorized disclosure, retention, or negligent handling of sensitive information and materials.

You are also verifying, by your signature, that you understand the consequences of breaching this Non-Disclosure Agreement.

REQUIREMENTS TO MAINTAIN YOUR CLEARANCE

In order to hold a clearance or special access, you need to meet some basic requirements.

- You must receive the initial security training, which you are doing now.
- To maintain your clearance you must have valid contract work that requires you to have access to classified material. You must notify your security representative when the contract you are working on changes or when your position and responsibilities change in a way that could impact you clearance/access requirements.
- You will continue Periodic Re-investigations depending on your level of clearance (ranging from five to ten year increments).
    - You may have to complete additional screenings such as a polygraph.
- You will always need to verify a need-to-know before releasing classified information.
    - Just because a person has a security clearance does not mean they have a need-to-know. It is your responsibility to determine that the person should know the classified information in performance of their job responsibilities.
- You are required to report adverse information to your security representative.
- You will participate in annual security refresher briefings and trainings.

CLEARANCES VERSUS ACCESSES

Clearances and accesses require sponsorship through the customer being supported. For DoD, this is achieved by identifying and maintaining alignment with classified contracts. For special access, this is achieved by identifying and obtaining customer sponsorship and approval.

There are three levels of classification within the Department of Defense (DoD), Confidential, Secret and Top Secret.

- **Confidential.** Confidential is information that when compromised could expect to 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.

If you received an Interim clearance level of either Secret or Top Secret you are authorized to access most classified material. There are restrictions with an interim level for some specific

classified materials such as NATO, CNWDI, SAPs, etc. Check with your local security representative to determine specific restrictions based on your particular job needs.

Clearances and accesses are sometimes used interchangeably however, they are very different. A person only holds one clearance at a time which is either, Confidential, Secret or Top Secret. However, an individual may hold multiple accesses simultaneously. They are coordinated through Special Access Programs (SAPs) or Sensitive Compartmented Information programs (SCI). Accesses provide more stringent levels of control on specific information related to intelligence sources, methods and technologies.

In addition to your clearance level, in order to provide the most stringent protection of information you should practice the need-to-know principle. This means that not only should you verify the clearance level of the person to which you intend to release information but also their need-to-know.

Ask yourself these questions:

- Is this person working on the project involving this information?
- Do they need the entirety of the information or only a small portion to complete their portion of the work?
- Do they understand the protection measures and distribution of the information being released?

Additional information about special accesses can be provided by your Site Security Representative.

WHO ARE WE PROTECTING

Our primary business is national security. So what are we protecting?

Our Nation. We are protecting our war fighter and people in countries abroad as well as our citizens here in the United States.

Our Company and Jobs. We must ensure strict adherence to rules and regulations set forth by our leaders to solidify the ongoing and future success of this company.

Our Customers and Suppliers. According to our CEO, their success is our success.

GOVERNMENT OWNED INFORMATION

There are two categories of government furnished information that require our protection.

- Unclassified

- Classified Information

Unclassified information, including For Official Use Only (FOUO) and Controlled Unclassified Information (CUI) should be secured in some manner at the end of the working day. This can be as simple as putting it in a desk drawer or as complicated as securing it in an approved safe or alarmed facility. Specific guidelines are available, be sure to check with your local Security Representative.

Classified information provided on a contract (Confidential, Secret or Top Secret, SI/TK, etc.), requires that individuals maintain positive control of material at all times. All government furnished materials, depending on the level, should be destroyed or returned to the customer when no longer needed or at contract completion. Coordinate with your local Security Representative for appropriate disposition.

Northrop Grumman is not permitted to disclose classified or unclassified information pertaining to a classified contract to the public without prior review and approval by the government customer. If you have a need to give a presentation or create brochures, promotional sales literature, reports to stockholders, or similar materials, on subject matter related to a classified contract, even if the final material will be unclassified, please submit your request though the Enterprise Public Release Online Clearance System (eProcs).

Classified information made public is not automatically considered unclassified. Northrop Grumman personnel shall continue the classification until formally advised to the contrary.

CATEGORIES OF COMPANY PROTECTED INFORMATION

Northrop Grumman employees must also protect company proprietary information. This information is divided in to two categories:

- **Level I information** - is information that reveals technical methods and applications that are unique to Northrop Grumman.
- **Level II information** - is information that is exclusive to our company and not publicly available, such as financial or strategic planning data.

When handling these types of information consider the value they could have to a competitor. These types of information should be destroyed by shredding or placed in approved areas for destruction of unclassified proprietary information. Never place proprietary information in common trash receptacles.

If you are not sure how you should handle company proprietary at your location, contact your local Security Representative.

TRANSMISSION AND DESTRUCTION OF PROTECTED INFORMATION

The transmission and destruction of protected information, regardless if it is company proprietary or customer classified or unclassified may have specific requirements. Before destroying or transmitting protected information, ensure you understand these requirements.

Details regarding transmission and destruction of **company proprietary** information is addressed in CO J300.

Consult with your site security representative for details regarding transmission and destruction of **classified, special access or protected customer unclassified information, material or equipment.**

PROTECTION OF INFORMATION

Protection of information is the key to our success and you are the primary factor in that protection. Immediately report actual or suspected information security incidents to the Cyber Security Operations Center, known as the CSOC, including:

- Lost or stolen company computers, cell phones and other electronic equipment
- Lost or stolen removable media, such as USB flash drives
- Suspected compromise of passwords
- E-mail acknowledgments or delivery receipts for actions you did not initiate
- System compromise, suspected compromise or unexplained system anomalies; and
- Spear Phishing and other suspicious email, including the suspicious e-mail as an enclosure.

Report suspected or actual loss or breach of Sensitive Personal Information (SPI) or contractually protected Personal Information (PI) to the Privacy Office at Privacy@ngc.com.

Report suspected illegal or inappropriate use of the internet or company computing resources to your immediate management, Business Conduct Officer, or the Northrop Grumman OpenLine.

Classified information CANNOT be entered into any computer or other electronic device at Northrop Grumman if it has not been formally authorized for classified processing. If you have any questions as to whether a system is authorized, please contact the Facility Security Officer (FSO) or Information Systems Security Manager (ISSM).

Through our processes and security controls, the company maintains the required high level of protection for classified information provided by or developed for U.S. government agencies. We must all be aware of the potential for classified information to be inappropriately introduced into the company's unclassified information systems, including electronic media. We term this a “Code Blue” event.

Immediately report an actual or suspected Code Blue to the Northrop Grumman Security sector Code Blue contact or other Security point of contact. If you are not able to immediately reach a Security point of contact, report the potential Code Blue directly to the CSOC at 877-615-3535. When reporting a Code Blue, do not disclose information which may be classified over unsecure channels. Act promptly to prevent further possible proliferation.

For more guidance refer to CTM J100, Chapter 3 – *Company Security Manual*

Links:

Cyber Security Operations Center (CSOC) (Monitored 24x7)
Email: CSOC@ngc.com Phone: 1-877-615-3535

NG OpenLine: Website: OpenLine (myngc.com)
Phone: 1-800-247-4952

Code Blue: Website: Code Blue (sharepoint.us)

THE BEST RESPONSE

- If someone asks questions that are sensitive, do your best to steer conversations to another topic.
- Avoid accessing internet sites that post speculative information.
- Do not confirm or deny classified validity of information found in open source materials, such as technical blogs and news reports.
- Classified information in the open press is still classified. You should never confirm, deny or comment on this type of information.
- If you see suspicious activity report it on the My Security website.

BADGING

Badges are required to be worn when inside any Northrop Grumman facility and should be visible between your shoulders and waist and in plain view. These badges not only say who you are, they also indicate your clearance level, access levels and citizenship.

- If a smart card is used for computer access, remove the badge from your computer system every time you step away.
- When entering any Northrop Grumman facility, no tailgating! Everyone must present their own badge or PIN to the card reader to confirm valid access. Please ensure the door closes behind you. See local security if you require access and your badge is not programmed.
- Remove your badge when exiting the facility to protect yourself from becoming an intelligence target.

- Politely challenge anyone without a badge and escort them to a Security Officer if unable to produce a badge.
- Report lost or stolen badges immediately.

If your clearance level is lowered or you are debriefed from special accesses, you should obtain a new badge immediately. Your Site Security Representative can advise if this action is needed.

VISITORS

Visitors into Northrop Grumman facilities should always check in with the designated visitor control.

Make sure if someone is following you closely when entering a facility or areas that require card access, to verify they have the appropriate badge.

If possible, coordinate your visitors with security in advance. If you need a customer or other visitor to have a no escort badge, coordinate this request with security.

If your visitor has an escort required badge this means that you will escort the visitor at all times. For instance, if you are in a meeting and the visitor needs to make copies, you or someone you designate will escort them to the copier, remain with them and escort them back.

Non-Northrop Grumman personnel are not allowed access to our network. This includes inserting thumb drives into machines. Not only does this protect Northrop Grumman but also protects the visitor.

Remember, foreign visitors require a Foreign Visit Request processed through Enterprise Export/Import Management System (EEMS).

INSIDER THREAT

“Insider threat” is the term used for the potential harm posed when an individual intentionally or unwittingly uses or exceeds access to negatively affect information or systems, or compromises our government customer’s mission.

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. A recent brochure on insider threats cited that in the 11 most recent cases, 90% used computers while conducting espionage and two-thirds initiated the contact via the Internet.

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 My Security 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 Example: Go with your Gut

Ana Belen Montes was recruited by Cuba after learning of her views against the U.S. policies towards Central America. At that time she was a clerical worker in the Dept. of Justice. She went to work for the Defense Intelligence Agency and became the DIA's top Cuban analyst.

While security officials became aware of her disagreement with U.S. foreign policy and had concerns about her access to sensitive information, she had passed a polygraph test.

According to a FBI news story, in 1996 "an astute DIA colleague – acting on a gut feeling – reported to a security official that he felt Montes might be under the influence of Cuban

intelligence." She was interviewed but admitted nothing.

Four years later when the FBI was working to uncover an unidentified Cuban agent, the security official recalled the interview and contacted the FBI. An investigation was opened that led to her arrest and conviction.

References:

- 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

The U.S. cleared industry is 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 Cyber Security Operations Center (CSOC) at CSOC@ngc.com or 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. 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 My Security 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 (CSOC) at CSOC@ngc.com. Report suspicious phone contacts to the My Security 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 officer 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.

Case Example: As Much Time as it Takes

In 2010, ten deep-cover Russian spies were arrested. The individuals in the group married, bought homes, and had children as they appeared to assimilate into American life while actively collecting information and spotting and assessing potential recruits.

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 My Security 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 please use that approved reporting method versus the process described here.

Reference:

References:

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

COUNTERINTELLIGENCE AND SECURITY REPORTING REQUIREMENTS – REPORTING REQUIREMENTS SPECIFIC TO THE PERSON

The Government is not looking for perfect people, but they are looking for people with high standards of honesty and integrity. Self-reporting is one way of demonstrating your commitment to maintaining these high standards.

You also have a legal obligation to report certain events and activities, not only about yourself but your coworkers to your Security representative. For a more detailed list review the Reporting Guidance found here.

These include:

- Loss, compromise or suspected compromise of classified information
- Known, or suspected security violations involving classified data
- Changes in personal status such as, name changes, citizenship, or when an employee no longer has a requirement for a security clearance
- Becoming a representative of a foreign interest, including work, or support for a foreign government, company, or individual.
- All business and personal travel outside the U.S.

You are also required to report information of an adverse nature not only about yourself but your coworkers. Adverse information such as:

- Arrest or detention by any law enforcement agency
- Financial situations, such as bankruptcy, garnishment of wages and excessive indebtedness. Or, unexplained affluence, such as a sudden wealthy lifestyle without an increase in salary and, money transfers inexplicable by legal sources of income.

- Uncontrolled use of alcohol, 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. Mandatory enrollment in our Employee Assistance Program, refusal to accept rehabilitation assistance when offered and incomplete or unsuccessful participation in a rehabilitation program are all reportable.
- Other matters which may have an adverse impact to safeguard classified or proprietary material.

Keep in mind that reporting adverse information is never the sole basis for suspending, revoking or loss of a security clearance. Your security representative acts on behalf of the government and you can be assured this information is kept in the strictest confidence. If you are not sure if information is reportable, check with your Security Representative for additional guidance.

ENTERPRISE SECURITY RESOURCES

For more information on various security matters, visit the Enterprise Security Website. It would also be helpful to view the Foreign Travel and Annual Security Refresher training. Click the Training tile on the bottom of the page. The Training page will be displayed. Click on the training you wish to view. To view your Security Leadership click the Org Chart link. To find your Security Representative click the Security Contacts by Location tile on the bottom of the page. Shown are Enterprise Security resource links for more information.

Travel Awareness:
https://lx.myngc.com/Saba/Web_spf/NA9P1PRD001/common/registercatalog/dowbt000000000004865

Annual Security Refresher Training: Annual Security and Computer Refresher Trainings | Northrop Grumman

Cyber Security Operations Center (CSOC): CSOC@ngc.com / 877-615-3535 (monitored 24x7)

EMPLOYEE BADGE

Once we receive notice of the completed initial briefing and your signed Standard Form 312, Non-Disclosure Agreement, we will enter it into our system. You will be able to receive an updated Northrop Grumman employee badge which will indicate your clearance level. Contact the Badging Office copied on the e-mail you received to request your new One Badge.

DERIVATIVE CLASSIFIER TRAINING

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.

You will be assigned derivative classifier training after completing this training and returning your Standard Form 312.