Welcome to your annual security refresher training. The purpose of this briefing is to remind you of your personal responsibilities and liabilities under United States espionage and sabotage acts, and to reaffirm key security policies and procedures.
Today's business at Northrop Grumman is as diverse as our people. Each of us has a unique goal and mission within the enterprise. However, one responsibility that we all share is the obligation to protect and secure the information that we have access to in performing our job duties.
When you received your security clearance, you signed a non disclosure agreement form. By signing this form you agreed to:

- Accept a lifelong obligation to protect classified, SCI and sensitive government information.
- To submit any writing for a pre-publication review.

You vowed to avoid unauthorized disclosure, retention, or negligent handling of sensitive materials.

You also verified, by your signature; that you understood the consequences, of violating this non disclosure agreement.
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.

This annual refresher training is provided to you as a protection measure and reminder of appropriate handling measures, your obligations, reporting requirements, and responsibilities as a cleared employee, and as a result of this agreement.

For more information on these titles, visit the websites shown.

Title 18: [http://uscode.house.gov/browse/prelim@title18&edition=prelim](http://uscode.house.gov/browse/prelim@title18&edition=prelim)
Title 50: [http://uscode.house.gov/browse/prelim@title50/chapter23&edition=prelim](http://uscode.house.gov/browse/prelim@title50/chapter23&edition=prelim)
There are two categories of government information that you may deal with at your current job responsibilities.

**Unclassified** – is material that does not require a security clearance and,

**Classified** – material that does require special clearances and considerations to have access.
Unclassified material can be very sensitive information to our company and your job duties. In some cases, the material may have special handling and destruction requirements. Unclassified material that is co-mingled with classified material must be marked unclassified.

This type of data will normally be marked For Official Use Only (FOUO). Another unclassified marking is Controlled Unclassified Information (CUI). These types of information are not for public disclosure.

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, check with your program manager, supervisor, or contracting officer, if you have materials that contain these types of marking labels.
There are three distinct levels of classification within the Department of Defense system.

- **Confidential** – is information, that when compromised could expect to cause damage to our national security.
- **Secret** – is information, that when compromised, could result in grave damage to our national security.
- **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. Employees are responsible for familiarizing themselves with the classification guides and directives associated with the program they are supporting. When creating a classified document it is the originator's responsibility to determine the appropriate classification level. When you are unsure how to interpret the classification guide, discuss with your supervisor or manager. Classification guides are available from your program security office.
When creating classified material be aware that there are two types.

- Originally classified, is that material classified by a government official, designated in writing by the president of the United States, based on the recommendation of the Director of the Information Security Oversight Office or the Original Classification Authority (OCA).
- Derivatively classified material. As a cleared contractor employee, that creates classified materials you are considered a derivative classifier. This means that classified material created is derived by a source document or documents, or from guidance provided by a security classification guide or government directive form known as a DD 254.

If an employee believes that information is classified improperly or unnecessarily, the classification may be challenged, or a determination made through program security and the government contracting agency or original classifying agency. In addition, as a holder of these materials, you are required to limit access to the information to those that have a need to know. By enforcing this, need to know principle, you will limit the chances that the classified information, could be compromised through inadvertent disclosure or release, and in turn keeps our nation and its secrets more secure.
Another type of protected information is our own company proprietary. This information is divided into 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 materials should be destroyed by shredding or placed in approved areas for destruction of unclassified proprietary information. If you are not sure how you should handle company proprietary at your location, refer to the Protection of Company Information pamphlet or policy CTM J301, located on the Corporate Security Website, or contact your local Security representative.

HELPFUL LINKS:
- Protection of Information Procedure: [https://home.myngc.com/sites/CommandMedia/Documents/ctmj301.docx](https://home.myngc.com/sites/CommandMedia/Documents/ctmj301.docx)
- Proprietary Information Protection Web Page: [https://ess.myngc.com/Security/Pages/ProtectionInfo.aspx](https://ess.myngc.com/Security/Pages/ProtectionInfo.aspx)
- Level I and Level II Coversheets:
  - [https://home.myngc.com/sites/CommandMedia/Forms/c-201.pdf](https://home.myngc.com/sites/CommandMedia/Forms/c-201.pdf) (Level I)
The first known collection efforts occurred several hundred years ago, and continue today. In recent years collection efforts have become more focused on dual use technologies. Reports indicate that the extent of foreign interest in specific categories of technology varies dramatically from country to country, and the leading edge technologies are not the only technologies being targeted. Countries with less developed industrial sectors often prefer older, off the shelf hardware and software that costs much less and is more suitable, for integration into their military programs. This lends additional credibility to using care when providing information to foreign nationals, since you may not always be aware of its end use.
Fiscal Year 2014 saw a continued increase in reported foreign collection attempts to obtain sensitive or classified information. The number of reports submitted to DSS rose to over 34,000 (an 8% increase from FY13). The six collector regions remained in the same relation to each other as well as the top five targeted technology sectors; 1) Electronics, 2) Command, Control, Communication, and Computers, 3) Aeronautical systems, 4) Software, and 5) Marine Systems. Each region legend illustrates the percentage of reporting associated with that region; the threat level DSS attributed to the region; the percentage of change in reporting compared to FY13; and the top technologies, methods of operation, and collector affiliations. Regions and categories are listed in order of prevalence based on overall FY14 reporting. To view the complete report click here: http://www.dss.mil/documents/ci/2015_DSS_Trend_Report.pdf.
The American society of Industrial Security recently conducted a survey of trade secret theft. This survey found, that the most common targets were customer related information, such as:

- Business volume and preferences
- New product information
- Financial data
- Manufacturing process information.

Use caution when sharing these types of information during times you may be working with our competitors.
Our diligence in exercising the need-to-know principle, by restricting access to the material you possess, plays a key role in the prevention of potential espionage. Most spies reported that they were able to obtain more information than they were initially seeking.

Always maintain direct control of classified and sensitive information and mark materials properly.

Review your holdings annually for proper disposition and keep retention to a minimum. This will cut costs by dealing less with the storage and maintenance of materials.
Visitors to Northrop Grumman facilities will have different requirements based upon the clearance level of the visitor, the status of the visitor, such as citizenship and program involvement, as well as the restrictions required by that specific area.

Visitors will be assigned either a No Escort, or Escort required badge based on the requirements mentioned earlier. As a sponsor for a visitor, you should ensure that your visitor understands any restrictions or requirements placed upon their visit to the facility. If your visitor is assigned an Escort required badge you are responsible to ensure the individual is within your line of sight at all times during the visit. You must also prevent the visitor from having unauthorized access to information. All foreign visitors must be coordinated and approved by Export Compliance prior to the visit. For specific requirements about signing in a visitor to your site or classified area check with the security officer primarily responsible for that area.
As the meeting host you are responsible to ensure prior to dissemination of any classified information that:

- The location is secure and discussions are not able to be overheard.
- All attendees have the appropriate clearance and access levels.
- All attendees have a need to know the information.
- All electronic devices are removed or powered off depending upon site and program procedures.
- And, prior to beginning any classified discussions, set and announce the level of the meeting.

As a reminder you should never process classified information on an unclassified system. Coordinate with your security representative if a classified computer is required.
Classified information in the open press is still classified. You should never confirm, deny or comment on this type of information.

After all, you are recognized as a knowledgeable expert, and comments you make, could be very damaging to you, personally, as well as the company.
When attending trade shows, as an exhibitor or a guest, be aware that everyone there may not have your best interest in mind.

Information, or sensitive equipment, may be stolen, so that it can be copied through reverse engineering. For some purposes, it may be sufficient to only gain access to the equipment for a brief period.

Avoid giving out too much information, instead provide just enough to gain interest, but still maintain our competitive edge.

All information, that will be made public, requires approval prior to its release.
When utilizing your company computer on the internet, don't draw attention to yourself, or your clearance by surfing foreign intelligence sites, or sites that are fishing for individuals with a specific clearance level.

Be careful what you download. If you must download a file or application, make sure it's from a trusted and secure site. Avoid accessing sites that post speculative information.

And, above all, remember, there is no security on the internet.
As an employee of a Government Contractor, you should not avoid contact with foreign nationals, or distrust all persons from abroad. Your encounters with foreign colleagues and cultures should be among your most treasured experiences. However, you must always be aware, that among the millions of foreigners who come to our country, or whose countries you visit, there are some who would exploit your trust.
As you follow your career path, you may find that you somehow stumbled on the road to recruitment, where foreign agents are targeting you. Along this road, there are several stops. All of which are designed to establish and maintain a relationship.

- The first stop is the **initial contact**. The foreign agents plan is to confirm whether or not you have information of value. If confirmed, they will establish a logical basis for continuing contact and obtain your agreement to meet again.

- The next stop is the **operational contact**. The foreign agent will look for some sort of vulnerability. In other words, they will determine if you are worth the effort of spending valuable time and money. Now is the time to report it to your security officer.

- If you continue on, your next stop is **developmental contact**. At this point, the foreign agent's goal is to establish a relationship of friendship and trust. This may cause you to feel a sense of obligation. The foreign agent will start asking for simple things, such as, professional advice or information about a co-worker. After the trust is established, they will request your company's internal phone book or proprietary documents about what your company has developed. You have now become a trusted source. You are willing to provide the foreign agent with any information they ask for. They have put you in a compromising position and know you are too afraid to report to your security office.

If you find yourself on the road to recruitment, and think you are a target, inform your security officer immediately. It's never too late to report it.
Dealing With Suspicious Requests

Your main defense against espionage is awareness and reporting all suspicious contacts to your security office. If you inform security, we can alert you when you are dealing with a known foreign intelligence operative or we may help you identify an agent. If you do find yourself in contact with a suspicious person or foreign intelligence operative, no need to panic but remember to use caution. You are much more likely to be charmed by a friend than blackmailed by an enemy.

If the contact goes so far that you are asked to provide information, perhaps as a consultant, you should:

- Listen carefully
- Be observant
- Remember as many details as possible
- Keep all options open by neither agreeing or refusing to cooperate
- Remain calm
- Be non-committal
- Ask for time, and
- Report immediately to your Security office.
Cleared employees have a legal obligation to report certain events, not only about yourself but your coworkers. 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, marital changes, citizenship, or when an employee no longer has a requirement for a security clearance.
- On becoming a representative of a foreign interest, including work, or support for a foreign government, company, or individual.

You are also required to report information of an adverse nature. 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.
- Other matters which may have an adverse impact to safeguard classified or proprietary material.

Your Security officer 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 officer for additional guidance.
Unfortunately, when dealing with classified information there can be security incidents, infractions or violations. Types of these that occur most frequently are:

- Classified area left unsecured
- Allowing an uncleared individual into an area
- Introduction of prohibited items
- Classified material removed without proper authorization; and
- Data spillage
  - Pay attention when using unclassified computer systems
  - Know what is classified. Become familiar with the classification guide.

Employees must report any non-compliance or willful/gross neglect of security requirements or procedures. Employees are encouraged and expected to report any information that raises doubts about another employee's continued eligibility for access to classified information. Report any information regarding actual or potential acts of espionage, sabotage, or terrorism.
End-of-the-Day Security Checks

Conducting an end-of-the-day security check of your work area helps to:
- Ensure that all information systems are shut down, or password protected and locked.
- Ensure that all classified material is properly stored and protected.
- Ensure that all storage containers and closed areas are properly secured and alarmed.

If you are asked to participate in the end of the day security check, please do so. This inspection plays a key role in our in-depth Security program and the protection of our nation’s information.
Another way, that we protect our nation’s information, and our company’s competitive edge, is by requiring a badge be worn when inside any Northrop Grumman facility.

- Always wear your badge in plain view and above your waist.
- Remove your badge from your computer system, every time you step away from your work area.
- Remove your badge when exiting the facility, to protect yourself from becoming an intelligence target.
- Politely challenge any one without a badge, and
- Report lost or stolen badges immediately to Security.
Compliance with security requirements is an ongoing part of your position. The purpose of reporting possible compromises is to detect and correct any vulnerabilities that might have been caused, due to the compromise. Security vulnerabilities or compromises may require reports to the customer.

Negligence that results in a security violation may receive disciplinary actions. These actions are on a graduated scale, which may include, depending upon the severity, verbal or written reprimand. Continuing security issues may affect your employment. For more information consult with your local Security department.
A reporting hotline program is active at Northrop Grumman, and within the Department of Defense. The purpose of the OpenLine is to provide an opportunity to report instances of fraud, waste, abuse of authority, and mismanagement. 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 provided hotline. Remember, comments and questions made during these contacts must be kept unclassified.

For additional guidance on the OpenLine and Government hotline procedures, please contact your local Security representative.

If your report deals with a special program that you are working please use that approved reporting hotline method versus the numbers explained here.

Government e-mail: hotline@dodig.osd.mil   Web: http://www.dodig.mil/hotline
The Security program provides protection for classified and sensitive information, and ensures that only authorized persons are permitted access to our information. We utilize, “Security in-depth,” which involves protection items such as: facility alarms, identification badges, visitor control, classified safes, closed room access control, and many others.

While any one of these security measures represents a strong barrier, our most valued partner is...YOU. Remember, Security is a team effort and an individual responsibility. The Security organization, is counting on you. Thank you for your time and effort in helping make Northrop Grumman Security a superior program.
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 select the appropriate button (link) on the next slide and complete the additional training.

Please note, first follow the necessary steps to receive credit for viewing this security refresher training.
If you have any questions or comments, please contact your local Security representative, or call the Enterprise Security Shared Service at 1-855-737-8364 or 855-SERVE NG.

Please send an e-mail to: ESSS_DoDTraining@ngc.com stating you completed the Security refresher training. Also, in your e-mail, please include your legal first and last name, your MyID or last 4 digits of your social security number and the training code (IMTRND), shown on the bottom right corner to receive credit for your required refresher training.

As noted on the previous slide, if you are a derivative classifier, select:

- Inside NG Domain: LX site
- Outside NG Domain

To complete the additional training. To receive credit for viewing the security refresher training, please click the X in the upper right corner to close the window. This concludes your annual security refresher. Thank you and have a great day.