



# Security Briefing

**THIS BRIEFING IS UNCLASSIFIED**

This briefing satisfies the requirements of the National Industrial Security Program Operating Manual (NISPOM)

**UNCLASSIFIED**

# Topics



Need-To-Know

Clearance Levels

Combination Controls

Safeguarding Classified

Reportable Information

The Threat

Foreign Travel

Foreign Recruitment

Economic Espionage

Automated Information Systems

Badges/Security Color Code

Classified Visits

Export Compliance

Adverse Information

Think Defensively

Foreign Visitors

Security Violations

Counterintelligence

**UNCLASSIFIED**

# Classified Information



Classified information is information that, in the interest of national security, requires protection against unauthorized disclosure.

(Facility name here) is assessed annually on its security compliance performance and its ability to properly safeguard classified information. A positive rating on this assessment is critical in maintaining our facility clearance and continuing to do business with the U.S. Government.

UNCLASSIFIED

# Need-to-Know



**DEFINITION:** Need-To-Know is the determination by an authorized holder of classified information that another appropriately cleared individual requires access to the information in order to perform official duties.

## **KEY POINTS:**

If you have any doubt, check with your supervisor before releasing any classified information.

Possessing a badge that indicates a clearance does not automatically grant individuals a Need-To-Know.

When working with contractors, it is important to determine the degree of Need-to-Know BEFORE sharing program or project information.

The Need-To-Know principle applies to computers as well. Do not share your password with anyone. Always secure your system by logging out or locking your computer.

**UNCLASSIFIED**



## Need-to-Know – cont'd

- Your security clearance does not give you approved access to all classified information. It gives you access only to:

Information at the same or lower level of classification as the level of the clearance granted; and,

Information that you have a need-to-know" in order to perform your work.

- Need-to-know is one of the most fundamental security principles. The practice of need-to-know limits the damage that can be done by a trusted insider who betrays our trust. Failures in implementing the need-to-know principle can cause serious damage to our organization.
- Need-to-know imposes a dual responsibility on you and all other authorized holders of protected information:

**UNCLASSIFIED**

## Need-to-Know – cont'd



When doing your job, you are expected to limit your requests for information to that which you have a need-to-know. Under some circumstances, you may be expected to explain and justify your need-to-know when asking others for information.

Conversely, you are expected to ensure that anyone to whom you give protected information has a legitimate need to know that information. In some cases, you may need to ask the other person for sufficient information to enable you to make an informed decision about their need-to-know.

You are expected to refrain from discussing protected information in hallways, cafeterias, elevators, rest rooms or smoking areas where the discussion may be overheard by persons who do not have a need-to-know the subject of conversation.

You should report to your security office any co-worker who repeatedly violates the need-to-know principle.

**UNCLASSIFIED**

## Need-to-Know – cont'd



The responsibility for determining Need-to-Know in connection with a classified visit rests with the individual who will disclose classified information during the visit.

Visits that may require a Need-To-Know *certification* are usually non-contractual and may depend on the destination. If you are attending a symposium, follow the instructions given by the host. The security section of these instructions will be completed by the Security department, but the Need-To-Know section is typically completed by your government customer .

**UNCLASSIFIED**



# Clearance Levels

Clearances parallel DoD classification levels. It follows that access to classified defense information is contingent upon you having at least a comparable level of security clearance. The primary D.o.D. clearances are:

- ***Confidential***: Information which, in the event of unauthorized disclosure, could reasonably be expected to cause *identifiable* damage to the national security.
- ***Secret***: Information which, in the event of unauthorized disclosure, could reasonably be expected to cause *serious* damage to the national security.
- ***Top Secret***: Information which, in the event of unauthorized disclosure, could reasonably be expected to cause *exceptionally grave* damage to the national security.

UNCLASSIFIED

# Badges/Color Security Code



**UNCLEARED**

**SECRET**

**TOP SECRET**

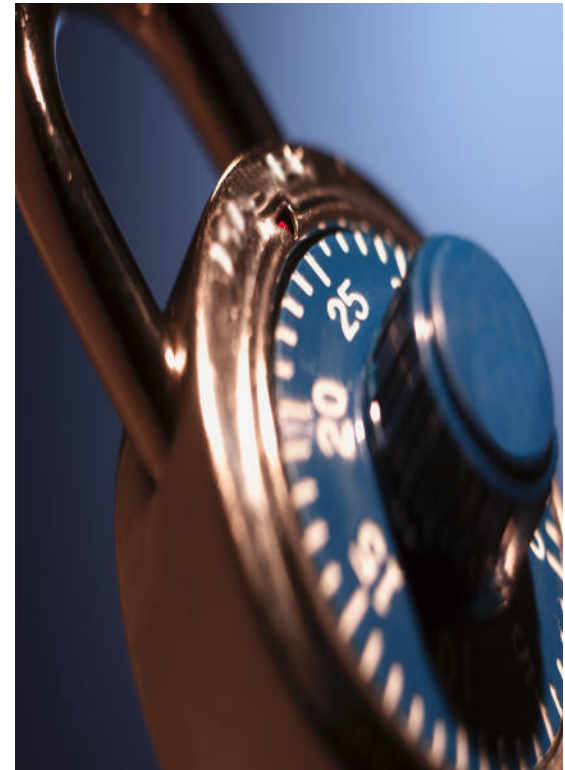
- Your badge shall be worn at all times while you are on facility premises.
- It shall be placed in a visible position, above the waist.
- If your badge becomes damaged or lost, report it to the Security Office immediately.
- The color strip located below your name signifies your clearance level.
- Badges shall be removed immediately upon exit of the premises.
- Piggy-backing on another employee's badge is a Security violation.
- If you notice a visitor or contractor in the building without a badge, contact Security.

**UNCLASSIFIED**



# Combination Controls

- Combinations which protect classified material shall be memorized, not written down.
- Combinations shall be changed upon initial issuance, when persons knowing the number have been debriefed, when the number is believed to have been compromised, or when otherwise deemed necessary by Security.



**UNCLASSIFIED**

# Classified Visits



## *Classified Visits*

### *Government and Contractor Visits*

- A Visit Request is required when planning a visit that will involve the disclosure of classified information to the Government or another contractor.
- Visit requests, both inbound and outbound, shall be forwarded to Security no later than 5 business days before the visit.
- International visitors shall allow at least 30 days notice for classified visits abroad.

UNCLASSIFIED

# Classified Visits – cont'd



## *Hosting a Visit*

Prior to holding a classified business meeting, *the host* shall verify that (facility name here) Security has received a *Visitor Clearance Letter* which includes the visitor's clearance information, purpose of the visit, and the appropriate need-to-know.



UNCLASSIFIED

# Classified Visits – cont'd



If you are the host of a classified visit, it is your responsibility to make certain that the visitor's clearance level is at least as high as the classified information being discussed.



**UNCLASSIFIED**

# Safeguarding Classified



When not in use, classified material shall be secured in a GSA-approved security container.

A locked room, desk or file cabinet is not an approved method of classified storage unless specifically authorized, in writing, by the Defense Security Service (DSS).

Containers shall be checked upon opening, closing, and at the end of the workday. Proof of checks shall be recorded on signature cards provided by the Security Department.



**UNCLASSIFIED**

# Safeguarding Classified – cont'd



## *Classification Markings - U.S. Government Mandated*

- *Security procedures require us to mark letters, reports, messages, data sheets, technical papers, and other material containing classified information.*
- *Classified items such as hardware, models, and videos shall also be properly marked.*
- *The markings are word symbols such as CONFIDENTIAL or SECRET, designed for clarity and uniformity and placed according to definite criteria.*
- *Cleared individuals who have responsibilities for creating/producing classified material shall comply with the guidance provided in DSSA Marking Classified Information, May 2006. This reference can be obtained on the DSS Home Page.*
- *Accurate classification of data is imperative. Contact Security if you have questions.*

**UNCLASSIFIED**

# Safeguarding Classified – cont'd



## *Transmitting Classified Information*

- Transmission of classified information by unsecured telephone, facsimile or any other method not approved by Security *is prohibited.*
- Hand carrying of classified material is prohibited unless written authorization is obtained from Security.
- All requests for transmission (incoming and outgoing) of classified material shall be coordinated through Security.



UNCLASSIFIED

# Safeguarding Classified – cont'd



## ***Reproduction of Classified Material***

Reproduction of classified data, photographs and artwork shall be coordinated through Security.

## ***Destruction of Classified Material***

Classified material that becomes outdated or no longer has reference value shall be destroyed. Upon making this determination, the classified material shall be brought to the Security Office for destruction. Non-Security personnel shall not destroy classified material unless specifically authorized by Security.

UNCLASSIFIED

## **Safeguarding Classified – cont'd**



- Foreign Government Information (FGI) material shall be controlled and brought into accountability. FGI material shall not be co-mingled with U.S. collateral material.
- If FGI and U.S. collateral material are stored in the same container, they shall be separated by folders and clearly marked.
- FGI shall be returned to the foreign government upon contract termination, unless the contract authorizes destruction.

**UNCLASSIFIED**

# Safeguarding Classified – cont'd



## *Retention*

- Classified information retained after the closing of a contract shall be destroyed. Authorization for retention may be requested of the customer, provided the information can be transferred to an active classified contract.
- If you do not have authorization to keep the material, it shall be brought to Security for destruction.

UNCLASSIFIED

# Safeguarding Classified – cont'd



NEVER divulge classified information to unauthorized personnel regardless of the passage of time, public source disclosure of data, changes in your clearance, access, or employment status.

UNCLASSIFIED



# Reportable Information

Cleared employees shall contact Security if any of the following apply:

- Name change.
- Change in marital status.
- Change in family status which results in having a foreign national as a relative.
- Reoccurring contacts with Foreign Nationals, or relationships with foreign businesses.
- Requests from anyone for unauthorized access to classified or export-controlled technical information.

**UNCLASSIFIED**



# **Adverse Information**

Adverse information is any information that adversely reflects on the integrity or character of a cleared employee. Such information would suggest that his or her ability to safeguard classified information may be impaired, or, that his or her access to classified information clearly may not be in the interest of national security.

It is the responsibility of all employees to report to Security any adverse information concerning another cleared employee.

**UNCLASSIFIED**



# Adverse Information

## *Examples of Adverse Information:*

- Criminal activity.
- Use of illicit drugs or misuse of controlled substances.
- Any pattern of security violations or disregard for security regulations.
- Excessive indebtedness/recurring financial difficulties.

UNCLASSIFIED



# Export Compliance

- Per the International Traffic in Arms Regulations (ITAR), Technical data in any form that pertains to the U.S. Munitions List (a list of defense-related articles) is “export controlled.”
- Access to, or disclosure of, such data to a Foreign Person is an export. U.S. Persons employed by Foreign Persons are generally treated as Foreign Persons themselves for the purpose of export compliance.
- In such a case, if the U.S. State Department has not issued an Export License (based on a Technical Assistance Agreement or Manufacturing License Agreement), a violation of ITAR has occurred.

UNCLASSIFIED

# Export Compliance – cont'd



## *Definitions:*

### **EXPORT**

- Shipping or transporting technical data or hardware out of the U.S.
- Transferring control or disclosing hardware, technical data, technology, software, electronic data to a foreign person (whether in the U.S. or abroad).
- Providing a Defense Service or Technical Assistance to a Foreign Person.
- Providing site visits/tours to Foreign Persons.

### **FOREIGN PERSON**

- NOT a U.S. Citizen
- NOT a U.S. Permanent Resident (e.g., Green Card)
- NOT a "Protected Individual" (e.g., Refugee or Asylee)

### **DEFENSE ARTICLE**

- An article or service that is specifically *designed, developed, configured, adapted* or *modified* for a military application and does not have predominant civil applications.

**UNCLASSIFIED**

## Export Compliance – cont'd



Export-controlled information or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulations (EAR). Export-controlled information must be controlled as sensitive information and marked accordingly. A large, frequently updated database of information on export regulations is available at [www.bis.doc.gov](http://www.bis.doc.gov).

UNCLASSIFIED

# Export Compliance – cont'd



- One objective of the ITAR and EAR is to prevent foreign citizens, industry, or governments, or their representatives, from obtaining information that is contrary to the national security interests of the United States.
- Different laws and regulations use different definitions of a U.S. person, U.S. national, and foreign national. This is a source of considerable confusion in implementing international security programs.
- The rules are especially confusing when dealing with an immigrant alien who possesses a green card for permanent residence in the U.S. For the purpose of export control regulations, such an individual is a "U.S. person" and *can* be allowed access to export-controlled information without an export license. If the export controlled information is classified, however, the regulations for release of classified information apply. According to the National Industrial Security Program Operating Manual, a permanent resident with a green card is still a foreign national and *not* a "U.S. person." Therefore, such an individual *cannot* have access to classified export-controlled information.

UNCLASSIFIED

# Export Compliance – cont'd



## **Access to Export-Controlled Information :**

Export-controlled information may be disseminated only to U.S. citizens or immigrant aliens. It is important to note that discussion with a foreign national in the United States, or a person "acting on behalf of a foreign person," constitutes an "export" if it reveals technical information regarding export-controlled technology.

## **Marking Export-Controlled Information:**

All documents that contain export-controlled technical data must be marked with the following warning:

**WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401 et seq.). Violations of these export laws are subject to severe criminal penalties.**

**UNCLASSIFIED**



# Export Compliance

ITAR violations can result in hefty fines and/or debarment from international business arrangements. Violations may also result in personal criminal liability. Prior to the export of technical data or hardware, contact the company Export Compliance Officer, (name here)

UNCLASSIFIED



# Automated Information Systems (AISs)

- All systems used for processing classified information including computers and test equipment shall be evaluated for NISPOM applicability. A formal approval is required by the Defense Security Service (DSS)/ODAA PRIOR to operating these systems.
- All classified processing shall be coordinated through the Facility Security Officer.
- Classified information processed on a non-approved system is a security violation which is reportable to the Defense Security Services (DSS).

UNCLASSIFIED



## **Automated Information Systems (AISs)**

- Do not connect a classified computer system to an unclassified system or network. In the event that this occurs, the unclassified system is considered contaminated. The classified information is then considered “potentially” compromised and an investigation will be conducted by Security.
- Notify Security immediately if you suspect that classified information has been processed on any non-approved system.
- Custodians and users of classified processing systems require special training and briefings.

**UNCLASSIFIED**

# Think Defensively



- Being mindful and thinking defensively will make it difficult for someone to obtain technical and/or classified information from you. As a (**company name here**) employee, you are considered to be a rich source of information by those people involved in both classic and industrial or economic espionage.
- Your increased awareness is essential when meeting with foreign nationals domestically and abroad or while vacationing outside the continental U.S. For current requirements and warnings for international travelers, visit <http://travel.state.gov>
- When you travel, refrain from discussing business in public places. Report to Security any suspicious contacts from individuals that you do not know.



**UNCLASSIFIED**



# The Threat

## Targeting of:

- Critical technologies
- Proprietary economic data
- U.S. officials
- National defense information

**Stockpiling of advanced weapons systems.**

**Obtaining technology for National economic gains.**

**Clandestine foreign intelligence activities.**

**Recruitment of U.S. citizens.**

**UNCLASSIFIED**



# The Threat – cont'd

## Who is a potential threat?

**ANY PERSON** who lacks proper clearance and a need-to-know, but still seeks to gain access to classified information. *This includes our nation's adversaries, as well as our competitors.*

*Examples:*

- Cleared/accessed employees
- Visitors
- Other defense contractors
- Overly curious family, friends or neighbors
- Foreign nationals
- Students

**Elicitation techniques are often subtle and difficult to recognize. Report all suspicious contacts to the Security Office.**

**UNCLASSIFIED**



# **COUNTERINTELLIGENCE**

FOREIGN RECRUITMENT

TRAVEL-RELATED VULNERABILITY

FOREIGN VISITS

**UNCLASSIFIED**

# FOREIGN RECRUITMENT



## WHAT IS RECRUITMENT?

An intelligence definition of recruitment is the attainment of someone's cooperation to provide sensitive or classified information, usually after careful assessment and patient cultivation of the target by an intelligence service. By the time the "pitch" (the offer to work for the foreign government) is made, the intelligence officer (the "recruiter") is relatively confident of the target's willingness to cooperate. If a failed recruitment attempt is reported, serious consequences may result for the involved Intelligence Officer (IO).

If the target agrees to the recruitment, that person becomes an "asset" or "agent", i.e. he has become a spy. The IO also called a "case officer," handles the asset by clandestinely receiving the information, paying his agent, and guiding the asset in his illicit activities. Why a person betrays his country is a complex issue, but money is almost always involved. Pursuit of financial gain often represents some other personal or psychological need such as ego enhancement, revenge, etc.

UNCLASSIFIED

# FOREIGN RECRUITMENT



Recruitment is usually a subtle and carefully orchestrated process to determine a person's receptiveness to working for a foreign government. If success is perceived to be possible, the pitch will eventually be made. Initially, an IO's interest in you may be imperceptible, but may become more obvious as the relationship develops.

Reporting questionable relationships, whether involving yourself, a co-worker, supervisor, neighbor, family member, or friend, is crucial to effective intervention. Espionage is never a "victimless crime." It damages lives and threatens the security of this nation. Notify Security should you have any indication that the company or any of your co-workers may be the target of an attempted exploitation by a representative of another country.

**BOTTOM LINE: BE ALERT... BE AWARE... REPORT SUSPICIOUS OCCURRENCES!**

UNCLASSIFIED

# FOREIGN TRAVEL



## OVERSEAS TRAVEL

Overseas travel increases the risk of being targeted by foreign intelligence activities. You can be the target of a foreign intelligence or security service at any time and any place; however, the possibility of becoming the target of foreign intelligence activities is greater when you travel overseas. The foreign intelligence services have better access to you and their actions are not restricted when they are operating within their own countries. Information Age spying includes:

- wired hotel rooms
- intercepts of fax and email transmissions
- recording of telephone calls/conversations
- unauthorized access and downloading, theft of hardware and software
- break-ins and/or searches of hotel rooms, briefcases, luggage, etc.
- bugged airline cabins
- substitution of flight attendants by spies/information collectors.

UNCLASSIFIED

# FOREIGN TRAVEL



## FAVORITE TACTICS

The overseas traveler and the information in their possession are most vulnerable when on the move. Many hotel rooms overseas are under surveillance. In countries with very active intelligence/security services, everything foreign travelers do (including inside the hotel room) may be recorded. These recorded observations can then be analyzed for personal vulnerabilities (useful for targeting and possible recruitment approaches) and/or useful information (collections).

UNCLASSIFIED

# FOREIGN TRAVEL



## FAVORITE TACTICS

A favored tactic for industrial spies is to attend trade show/conference type events. This environment allows them to ask a lot of questions, including questions that might seem more suspect in a different type environment. One estimate reflected that one in fifty people attending such events were there specifically to gather intelligence.

UNCLASSIFIED

# FOREIGN TRAVEL



## COMPUTER SECURITY

Another area of concern while traveling is computer security. Foreign Intelligence Services are not usually fortunate enough to have information simply dropped into their hands. They rely on tactics such as stealing laptops. These portable systems may contain access capabilities that serve as doorways to additional information and systems. In addition to theft, travelers have reported unauthorized access, attempted access, damage and evidence of surreptitious entry of their portable electronic devices.

UNCLASSIFIED

# FOREIGN TRAVEL



## COMPUTER SECURITY

Effective countermeasures to the aforementioned vulnerabilities include but are not limited to the following:

- Refrain from bringing portable electronic devices unless it is mission critical
- Use of removable hard drives
- Maintain personal cognizance of portable electronic devices
- Data on portable electronic devices should contain only what is needed for the purpose of your travel

UNCLASSIFIED



# FOREIGN VISITS

**International visits are a common part of everyday business in today's international market/economy and are a welcome opportunity to boost any business. The cleared Department of Defense (DoD) Contractor is no exception to this growth in the International Market. Visits to DoD Cleared Contractors by foreign delegations and individuals have been noted as one of the most frequently utilized modus operandi for targeting US Defense Industry for the past five years in the Defense Security Service publication, Technology Collection Trends in the US Defense Industry.**



**UNCLASSIFIED**

# FOREIGN VISITS



## TECHNIQUES

Remember, it is always cheaper for any country to elicit, improperly obtain or buy a new technology or the means of producing a new technology than it is for them to pay for the research and development (R&D) themselves. There are more funds expended on R &D by the US Government and Industry than any other country in the world, making US Contractors a prime target for collection of both classified and commercial/proprietary technology by foreign countries. There are several techniques and indicators to be aware of when a foreign visit is to take place at your facility. While hosting the visit, watch for any of the following techniques to help you decide if there is the potential for you to be targeted by the foreign visitor.

UNCLASSIFIED

# FOREIGN VISITS



## TECHNIQUES

- Peppering - Several of the visitors asking the same question in different styles or one visitor asking the same question to multiple US Contractor employees.
- Wandering visitor - The visitor uses the distraction provided by a large delegation to slip away, out of the control of the escort.
- Divide and Conquer - The foreign visitors take the US team members into different areas to discuss issues, thus, relieving the US person of his safety net of being assisted in answering questions or eliminating oversight of what he releases.
- Switching visitors at the last minute – A tool that is sometimes used to add a collector to the group without leaving enough time for a background check to be performed on the new visitor.
- Bait and Switch - The delegation says they are coming to discuss business that is acceptable for discussion, but after they arrive their agenda switches to different questions and discussions.
- The distraught visitor - When the visitor does not have questions answered he/she has a temper tantrum or acts as though they are insulted, thereby trying to get the US person to answer the questions and not be upset.

**UNCLASSIFIED**

# The Law



**It is against the law to:**

- **Disclose classified information to unauthorized persons.**
- **Fail to report a known or suspected compromise of classified information.**
- **Destroy National Defense Material without proper approvals.**



**UNCLASSIFIED**

# The Law



**Penalties for unauthorized disclosure of classified information can include significant monetary fines and life imprisonment.**

**There is NO statute of limitations regarding the unauthorized disclosure of classified information.**

**Espionage Law Title 18 - Sections 793, 794, 798**

**UNCLASSIFIED**



# Economic Espionage Act of 1996

- **The Economic Espionage Act (EEA) specifically proscribes the various acts defined under economic espionage and addresses the U.S. national and economic security aspects of the crime. The law also addresses the theft of trade secrets where no foreign involvement is found.**
- **As defined in the Economic Espionage Act of 1996, the term trade secret refers to all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:**
  - 1. The owner thereof has taken reasonable measures to keep such information secret;**
  - 2. The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public; and,**
  - 3. The owner of a trade secret is the person or entity that has rightful legal or equitable title to, or license in, the trade secret.**

UNCLASSIFIED



## Economic Espionage Act of 1996

- The EEA contains two separate provisions that make the theft or misappropriation of trade secrets a federal criminal offense. The first provision, under Section 1831, is directed toward foreign economic espionage and requires that the theft of a trade secret be done to benefit a foreign government, any instrument of a foreign government, or foreign agent. In contrast, the second provision, under Section 1832, makes the commercial theft of trade secrets a criminal act regardless of who benefits.
- Reflecting the more serious nature of economic espionage, a defendant convicted for violating Section 1831 can be imprisoned for up to 15 years and fined \$500,000 or both. Corporations and other organizations can be fined up to \$10 million. A defendant convicted for theft of trade secrets under Section 1832 can be imprisoned for up to 10 years and fined \$500,000 or both. Corporations and other entities can be fined no more than \$5 million.

UNCLASSIFIED



## **Economic Espionage Act of 1996**

The EEA is a powerful deterrent and is a very important law enforcement and security management tool for protecting intellectual property rights. The EEA is not intended to convert all thefts of trade secrets into criminal cases; however, the EEA substantially raises the stakes in the arena of economic espionage. To report violations of the EEA or to obtain additional information, contact Security.

**UNCLASSIFIED**



# Security Violations

- Security Violations are acts or omissions that violate established security procedures developed to protect classified information. A violation may or may not result in the loss or compromise of classified information.
- A security violation is also a violation of the Company's Standards of Conduct, which may result in disciplinary action to include suspension, termination and/or criminal prosecution. (if applicable)
- Security Violations are costly, but preventable.
- Report immediately!

UNCLASSIFIED



# Questions?

Questions regarding the information contained or referenced in this briefing should be directed to:

FACILITY SECURITY OFFICER  
TELEPHONE NUMBER: \_\_\_\_\_



**UNCLASSIFIED**



## Certificate of Training

(Input your employee information here)

**UNCLASSIFIED**