☎ TELEPHONE CONCERNS

You probably use standard DON secure and unsecure telephones and fax machines. Standard security procedures dictate the types of information you can discuss or transmit on each. However, when someone calls to discuss classified or sensitive information or asks for a fax, you must also ensure there is a need to know the information. Follow the same routine as if you were speaking face-to-face. Do not try to talk around classified or sensitive information.

YOUR RESPONSIBILITY

You, along with every person associated with DON, share the requirement to protect classified, sensitive, and proprietary information. Your personal responsibilities include using all of the available security tools, such as secure phones, faxes, safes, and badges, and learning the security skills needed to succeed in a high-security environment. One of these skills is the ability and courage to ask for sufficient information to enable you to make an informed decision regarding a person's need to know. Remember, not every cleared person who casually asks you about your job is a spy, but continued questioning regarding classified or sensitive information where an obvious need to know does not exist may be a security concern. If you notice this behavior, discuss it with your supervisor or security officer. Remember the need-to-know principle was developed as a personal security measure to prevent unauthorized disclosures of classified and sensitive information. Let's use it!

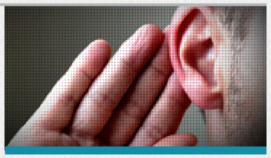
MAR13

NEED-TO-KNOW: SECURITY PRINCIPLE

NCIS

WWW.NCIS.NAVY.MIL

WHO NEEDS TO KNOW?



YOUR ROLE

You, as an authorized holder of classified, sensitive, or proprietary information have the authority and responsibility to ensure that sensitive and classified information is protected from inappropriate access. You need to confirm that people requesting information have the appropriate security clearance or access and that the information is needed for them to perform their official functions.

Need-to-know is one of the most difficult security principles to apply. The FBI estimates that 80% of espionage is committed by insiders. Most insiders who committed espionage were fully cleared, and some had access to special program information. In almost every case, these insiders gained access to information not pertinent to their jobs by circumventing the need-to-know principle, most often employing “social engineering” methods to disguise their actual, clandestine intentions. Social engineering is the art of preying on natural human tendencies to trust and help others in order to obtain information that would otherwise be hard to get.

In many cases of espionage committed by an insider, the perpetrator was successful because colleagues were hesitant to report potentially significant security issues, such as unreported or concealed contacts with foreign nationals, attempts to gain new accesses without a need to know, and failure to report overseas travel. Three espionage cases that dramatically illustrate the need-to-know breakdown are the cases of Jonathan Pollard, Aldrich Ames, and Robert Hanssen. Pollard, a Naval Investigative Service counterterrorism analyst with responsibility for the United States and Caribbean basin, was able to easily obtain documents on virtually any subject related to the Middle East and Far East from various intelligence agencies. Pollard was convicted in 1985 of selling classified material to an element of the Israeli intelligence service and was sentenced to life imprisonment. Ames was a CIA operations officer who, when arrested in 1994, had in his possession more than 100 documents related to U.S. intelligence operations in the former Soviet Union. Hanssen, an FBI counterintelligence officer and 25-year FBI veteran, was arrested in 2001 on suspicion of conspiracy to commit espionage on behalf of Russia and the former Soviet Union. He took advantage of security lapses and repeatedly used his position as a special agent to “bully” others to gain access. Hanssen’s transgressions and flagrant misuse of need-to-know resulted in the FBI initiating bureau-wide security changes that are still in effect today.

?? A FREQUENT DILEMMA

In the conduct of your daily duties, you may run into situations that make you question whether someone has a need to know certain information you have. For example, you are involved in a very sensitive DON special project or operation that a person from the office next door inquires about. You know many DON employees are cleared to top secret. Do you grant access immediately, decide quickly there is not a need to know and say so, or say that you will get back to the person when you have more information? You should ask the reasons for requesting access. If you are not convinced of a legitimate need for the information, deny access until you determine there is a need to know, or seek guidance from your supervisor or security officer. Determination of need-to-know is the personal responsibility of everyone. If there is any doubt as to someone’s need to know, ask your supervisor or security officer before granting access to any classified or sensitive information.

SPEAKING WITH CARE

The rumor mill is an area where you may overlook the need-to-know principle. You like to talk about your work, especially within DON, where you know “everyone” is cleared. However, areas where people from various offices congregate can lead to innocent chit-chat revealing sensitive information. Even though you know a person is cleared, either because of a badge or from personal recognition, that person may not need to know everything you feel like discussing. In short, look around every meeting place to be sure everyone has the required need to know before speaking.

COMPUTER CONCERNS

The need-to-know principle also applies to computers and computer media you use at work. Passwords you use to access DON, DoD, or other government automated systems are yours exclusively and should never be shared with co-workers. Always secure your computer by logging off or locking it before leaving an area for an extended time and secure authorized removable media. Ensure hardware is classified to reflect the highest level of information that is processed on the system. Related media must also be protected at that level. Always take time to affix classification and data descriptor labels and secure the media when finished. When you give media to someone else, be sure it contains only information that person has a need to know.