

Need-To-Know

Narration Script

Need-To-Know is one of the most fundamental security principles. According to the DoD 5200.2-R, need-to-know is defined as:

“A determination made by a possessor of classified information That a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program.”

The practice of need-to-know limits the damage that can be done by a trusted insider who goes bad.

Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual’s office, position, or security clearance.

Notice that the responsibility to determine “need-to-know” is the responsibility of the individual who possesses the classified information.

As someone who works with classified information, it’s a decision you may have to face when you least expect it.

One reason to be constantly aware of “need-to-know” is that some trusted insiders have gone bad. When this happens, careful observation of “need-to-know” helps to limit the damage. When someone looks for information that they don’t need-to-know, it may just be simple curiosity, but that is not the only possibility.

Here’s an example where it’s pretty clear that an insider was accessing material he didn’t “need-to-know” for nefarious purposes.

Leandro Aragoncillo grew up in the Philippines, immigrated to the U.S. and joined the U.S. Marines. During a successful military career he was appointed the staff assistant to military advisors in the Office of the vice president. At a White House function he met the president of the Philippines, Joseph Estrada, who pocketed his business card.

Some time later, after Estrada’s presidency collapsed in scandal, he had an associate contact Aragoncillo and ask for help saving the presidency. They appealed to Aragoncillo’s “Filipino patriotism”. Aragoncillo began stealing and passing along classified documents.

After Aragoncillo retired from the Marines, he began a new job as a civilian FBI analyst.

Now he ran unauthorized database queries on an FBI case management system and passed information about American political judgments, antiterrorist plans, and military actions to his continuing contacts in the Philippines. The queries were unauthorized because they were for information he had no “need-to-know”.

He sought out information that went far beyond what he needed to do his job. He used that information to betray his adopted country.

If Leandro Aragoncillo had asked you for information, would you have asked him why he needed to know?

Need to know can be really hard – it goes against our natural instincts and everything we have been taught about getting along in groups. Breakdowns in applying the need-to-know principle don’t usually stem from deliberate misbehavior. Instead, they arise from people trying to be helpful and cooperative – things we are taught to do from early childhood.

Need-to-know sounds so simple. The need-to-know principle says that having the clearance for information is only half of the issue.

The other half is having the need-to-know.

Individuals with authorized access to classified information are required to limit access to that information only to individuals whose clearance and need-to-know has been verified.

The need-to-know principle dictates that you, as an authorized holder of information, only share the information when two conditions are met.

These are:

One, the requester has the appropriate clearance and access.

Two, the requester needs to know the information in order to perform his or her job functions.

When both conditions are met, provide the information.

Verifying that the requestor has the appropriate clearance is usually straightforward. You see their badge, or know that the communication is coming through channels cleared at the appropriate level.

Verifying their need-to-know, on the other hand, may require some judgment. If it’s not clear to you that the requestor needs the information, then as program management.

When it comes to need-to-know, if you are an authorized holder of classified information, it is **your** responsibility to verify the need-to-know of anyone you want to share the information with.

Applying the need-to-know principle is a contribution to protecting national security that only you can make.

Remember:

Need-to-know imposes a dual responsibility on all authorized holders of classified information.

1. Limit your requests for information to that which you have a genuine need-to-know. You may be expected to explain why you need to know it.
2. Refrain from discussing classified information in areas where the discussion may be overheard by persons who do not have a need-to-know the subject of conversation.
3. If someone asks you for classified information, you are expected to ensure they are cleared appropriately and have an official need-to-know.

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