

COURSE 18, TUTORIAL 1

CLASSIFIED DOCUMENT GENERATION, STORAGE, AND CONTROL



Before we dive into this course, let's answer one basic question: Why do Small Business Innovation Research (SBIR) awardees need to be concerned about classified document generation, storage, and control? After all, the Department of Defense (DoD) SBIR program does not accept classified proposals. However, the truth of the matter is that during Phase II, it is possible that your work may go “dark” and your firm may be required to be able to handle classified information.

According to the DoD's **Defense Security Service (DSS)**, most of the technology developed for our nation's defense is produced by US industry. This is significant to you as a small business because a lot of the technology for defense is classified and therefore must be protected to ensure our national security. This brief course is intended to provide an overview of classified document generation, storage, and control. Needless to say, those involved in these activities must have obtained and hold a current security clearance and perform these activities in a cleared facility. This course does not address the process of obtaining a security clearance for personnel or facilities. Nor will this course address the specific contractor personnel requirements or the ongoing training and documentation needed to conduct these activities on an on-going basis. Our focus is strictly on classified document generation, storage and control.

NATIONAL INDUSTRIAL SECURITY PROGRAM

To carry out the task of securing and safeguarding classified technology, the government formed a partnership with private industry called the **National Industrial Security Program**

(NISP). Executive Order 12829 established the NISP to ensure authorized personnel protect classified information while working on contracts, programs, bids, or research and development (R&D). It is the responsibility of the DSS to administer the NISP for the DoD and 30 other federal agencies.

INDUSTRIAL SECURITY REPRESENTATIVES

One key element in the execution of the NISP is the DSS **Industrial Security Representative (ISR)**. They serve as the main liaison to cleared industry under the NISP. ISRs are located throughout the United States in four geographic regions and 48 field locations. Their job is to form a professional partnership with the contractor's facility management staff and facility security officer to ensure the safeguarding of classified information released under contractual obligations or through the process of R&D. When a small business/contractor has questions concerning classified or potentially classified information or documents, they can reach out to one of the DSS ISRs in their region of the country. The ISR will help the contractor comply with the **National Industrial Security Program Operating Manual (NISPOM)**.



GOVERNANCE



TRANSPARENCY



Industrial Security Representatives (ISRs) serve as the main liaison to industry through the National Industrial Security Program (NISP). The ISR helps contractors comply with the NISP Operating Manual (NISPOM).

NISP OPERATING MANUAL

The NISPOM is used by the US government's executive branch departments and agencies to control the authorized release of classified information to their contractors. It is the authoritative document for requirements, restrictions, safeguards, and procedures to prevent unauthorized classified information disclosure.

The president has ultimate authority for NISP but has designated the **Secretary of Defense (SECDEF)** as the program's executive agent. SECDEF consults with the affected agencies and gets the concurrence of the Chairman of the **Nuclear Regulatory Commission (NRC)** and the Director of the **Central Intelligence Agency (CIA)** on implementing and maintaining the NISPOM.

"The NISP applies to all executive branch departments and agencies and to all cleared contractor facilities located within the United States and its territories. This Manual applies to and shall be used by contractors to safeguard classified information released during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, perfor-

mance, and termination. It also applies to classified information not released under a contract, license, certificate or grant, and to foreign government information furnished to contractors that requires protection in the interest of national security."

CLASSIFICATION LEVELS

Among other things, you may be asking yourself "what does classification mean?" Basically, classification is a way of designating the importance of any piece of information as it relates to national security. There are only three classification levels or designations. They are **TOP SECRET, SECRET, or CONFIDENTIAL**. These terms are indicators of the relative importance of the information and its potential impact on national security if unauthorized disclosure of the information were to occur. **TOP SECRET, SECRET, or CONFIDENTIAL** are the only authorized designations for classified material and no other terms are permissible. Any information that does not require a security classification is designated as **UNCLASSIFIED**.

In the next tutorial, we will explore these classifications in detail and discuss markings.