

Modernizing the Secure Area

By: Isaac Fisher, Facilities Security Manager, Honeywell Aerospace

Secure Working Areas

When most people are asked to describe a secure room, we picture the secretive, high-tech areas from iconic spy films like *Mission: Impossible* or *James Bond*. We might imagine sleek, shiny walls equipped with retinal scanners and laser-activated motion sensors, which only the most daring secret agent would ever attempt to penetrate. In reality, modern secure areas often look like the spaces we work in every day: offices, conference rooms, laboratories and ordinary-looking places of business.

Each day, thousands of American service members, government employees and civilian contractors head into a secure area to perform vital work for our national security. There are over ten thousand secure areas across the private sector, including at businesses both small and large. These areas are designed to integrate seamlessly into the facility or business office environment. In fact, except for the strange-looking locks, heavy doors and the notable absence of personal electronic devices, most of us would not notice these secure working areas unless we were granted access.



Into the Vault: Ethan Hunt (Tom Cruise) infiltrates a highly secure room at CIA headquarters in the first film of the Mission: Impossible series (*Credit: Paramount Pictures*).

Types of Secure Areas

Contemporary secure workspaces are crafted to accommodate diverse levels of classified information and meet specific operational needs. The most common is the U.S. Department of Defense (DOD) Open Storage Area, or OSA. OSAs are designed to store and process collateral classified information for the DOD, such as the design or manufacture of sensitive military hardware. They are designed to safeguard this information from unauthorized disclosure, creating a safe and secure environment for verbal conversations, telephone calls, computing, document storage and even manufacturing environments. These areas are built to keep sensitive information safe and secure at all times, with reinforced walls, heavy doors, complex locking mechanisms and sophisticated alarm systems.

The most secure areas are designated as sensitive compartmented information facilities (SCIF) or special access program facilities (SAPF). SCIFs and SAPFs are designed and constructed to precise dimensions and tested to ensure they can safeguard the nation's most sensitive secrets from compromise. These areas take the security measures of the OSA even further, by preventing radio frequency emissions from escaping the room. Attention must be directed towards the construction of doorways, as well as the installation of electrical systems, air conditioning, and sprinkler systems. Once completed, the area essentially becomes a "Faraday cage", named for the English physicist who pioneered our understanding of electromagnetic energy in the 19th century. In fact, a properly-designed and constructed SCIF or SAPF is essentially a small fortress, immune to even the most sophisticated eavesdropping techniques.

Threats to Secure Areas: Electronic Intelligence (ELINT)

Throughout human history, nations and adversaries have gone to great lengths to gather information on their rivals' activities, plans, technologies and intentions. Early spies had to gain close access to collect information, observing their target or eavesdropping from nearby while remaining unseen. With [the advent of Morse Code in 1844](#), the world's first electronic messaging technology, a new era of human communication began. This transmission procedure promised to connect two distant ends securely, maintaining privacy while offering the convenience of near-instantaneous connection; however, it was not long before the system was first 'hacked': during a technology demonstration in London in 1903, rival inventor Nevil Maskelyne [intercepted and overrode the message](#) with his own transmission. For the first time, the world had reason to doubt the security and reliability of the budding electronic communications technology.

Over the following decades and to the present day, electronic communications have been the target of sophisticated, highly creative hacking, interception, jamming, spoofing and spying techniques. In many ways, electronic intelligence (ELINT) has become an art and a science of its own, employing tremendous human and technological resources across governments, including those of the [National Security Agency](#) of the United States. Virtually every major government across the world engages in some level of ELINT, which necessitates protection and safeguarding sensitive information from prying ears and eyes.



Electronic Eavesdropping: Adversaries can use a variety of techniques to intercept and collect electronic emissions from computer equipment (*Credit: Hackaday*).

ICD 705 Modernization

In January 2025, the Director of National Intelligence (DNI) released a memorandum requiring all SCIFs and SAPFs in the United States to meet the security requirements provided in Intelligence Community Directive (ICD) 705 (ICD 705) by the end of 2028. ICD 705 was first published in 2010 and has been revised and updated several times since. It is a publicly available document outlining the design specifications and security requirements for modern SCIFs and SAPFs.

The rationale behind the memo was made clear: the threat to U.S. national security has grown substantially since the original release of ICD 705 in 2010. Adversary nations such as the People's Republic of China and Russia have become significantly adept at intercepting electronic communications, circumventing security systems, and stealing critical information from our most sensitive locations. The risk has become too great to ignore, and U.S. firms must invest in modernizing their facilities if they wish to continue handling the most sensitive national security information. The release of the memorandum sent significant shockwaves through the U.S. defense industry, because it requires private firms to act quickly to modernize their legacy secure areas to remain compliant and continue using them. As one might imagine, the cost of constructing an ICD 705-compliant area is significant—several times that of a traditional office space. These factors, combined with the economic considerations of the inflated costs of materials, skilled labor and certain long-lead-time items, add up to a significant price tag for ICD 705 compliance. Most companies spent most of 2025 carefully evaluating their secure working areas, deciding which are critical to their operations and where to invest for future growth. Secure working areas offer an important lesson: national security is not protected by technology alone, but by the people who understand, design, maintain and respect these environments. As ICD 705 modernization reshapes the future of secure facilities, the next generation of professionals will play a critical role in balancing compliance, innovation, and operational needs. Learning the fundamentals of secure area requirements, electronic threats and facility modernization today can open the door to meaningful careers that directly support the protection of sensitive information and the nation's most critical missions.

