DTIRP Arms Control Security Information Article

A PRODUCT OF THE DEFENSE TREATY INSPECTION READINESS PROGRAM, DECEMBER 2007

Order Number 915A

The Risk of Inadvertent Technology Transfer

The United States is party to a number of arms control treaties and agreements that enhance global stability and increase cooperation and openness among its allies, economic competitors, and former adversaries. While all of these agreements support U.S. national security objectives, their implementation can increase the risk of inadvertent technology transfer.

Inadvertent technology transfer is the loss of critical information affecting national security and, potentially, the economic competitiveness of the United States. When preparing for an arms control inspection or an observation overflight, facilities must consider this risk.

Risk Environment

During arms control inspection activities, foreign nationals are unavoidably present at Department of Defense (DoD) and defense contractor sites and facilities. Their presence increases the risk of inadvertently transferring critical information, including scientific, technological, and economic information.

DoD sites and facilities identified or declared under treaty provisions, should conduct arms control operations security (OPSEC) analyses to identify risks and appropriate countermeasures. Declared facilities should also prepare inspection readiness plans to accommodate inspection activities.

Inspection preparation assistance and ongoing support is provided to defense contractor facilities through their Defense Security Service (DSS) Industrial Security representative or government sponsor. Facilities can also request assistance through DTIRP. By these means, declared facilities are generally well prepared to implement their inspection readiness plans when notified of an impending inspection.

When facilities are properly prepared, the risk of technology transfer during inspection activities is manageable. With advance planning and the proper use of treaty provisions, the inspectors' access can normally be negotiated or at least restricted to treaty-relevant areas and information sufficient for successfully demonstrating treaty compliance.

When assessing risks, it is important to remember that the inspection team will be composed of highly trained individuals who are experts in their fields. They will be capable of retaining everything they see, hear, smell, or sense.

Although the inspectors are often international civil servants representing an international treaty implementation organization and may be bound by secrecy agreements, the possibility of human intelligence collection and the transfer of sensitive technologies remains a security concern

Operations Security

To be prepared for on-site inspection activities, personnel at declared facilities need to conduct an arms control OPSEC assessment. This involves identifying critical information, analyzing the threat posed by the inspection team, determining the facility's susceptibility to inspection activities as specified in the treaty's provisions, analyzing vulnerabilities, assessing risks, and developing appropriate and cost-effective countermeasures when needed to protect national security, proprietary, and other sensitive information from inadvertent transfer.

What to Protect?

To protect critical assets and information during arms control inspection activities, the unclassified indicators of sensitive information need to be protected if they can be observed by the inspection team.

Some examples of potential indicators include:

- customer and supplier lists;
- financial data;
- innovative processes reducing operating costs;
- names of technical personnel working on a specific project;
- operating temperatures at key steps in a process;
- patent information;
- precise order and timing for materials to be introduced into a process;
- proprietary formulas for specialty chemicals;
- sensitive design elements; and
- the form, source, composition or substance of raw materials.

Protecting Sensitive Information

Protecting sensitive information while also allowing access to the areas and information needed to demonstrate compliance is the challenge facing facility staff each time an inspection team arrives.

The procedures and countermeasures employed to protect sensitive information during arms control inspection activities need not be expensive or elaborate. However, protective measures must be consistent with treaty provisions specifying the rights and obligations of the inspection team and those of the inspected State Party.

Appropriate and cost-effective countermeasures may be as simple and easy as turning a book around or turning off a computer monitor. Other security countermeasures and techniques that may sometimes be employed at U.S. facilities to deny or limit the inspection team's access to sensitive information and programs include, but are not limited to, the following:

- distance viewing;
- document redaction;
- route planning; and
- shrouding.

Depending on the technology to be protected and the level of access an inspection team may be allowed to have to the technology, facility staff may occasionally need to employ more costly or sophisticated materials and techniques. Being prepared in advance of inspection activities and conducting an arms control OPSEC assessment are key to successful site preparation.

Conclusion

DoD and other government agencies have hosted hundreds of foreign inspection teams as they have conducted arms control inspections at U.S. facilities in the United States and in Europe. The valuable lessons learned through this experience are continuously shared with impacted facilities and their government sponsors to assist facility personnel when preparing to receive inspection teams at their site.

For more information about the risk of inadvertent technology transfer and the application of security countermeasures, contact the DTIRP Outreach Program Coordinator at 1-800-419-2899 or send an email to dtirpoutreach@dtra.mil. You may also visit the DTIRP website at http://dtirp.dtra.mil or contact your local DSS industrial security representative or your government sponsor.