

Order Number 947A

The Arms Control Security Vulnerability Assessment Process

This article describes the purpose, personnel involved, and process of conducting arms control security vulnerability assessments. Vulnerability assessments focus on analyzing a facility's activities from the viewpoint of an inspection team sent to verify compliance with arms control treaty obligations. During the assessment, potential risks will be assessed and recommendations will be made about when, where, and how additional security countermeasures may be applied in relevant arms control environments.

Vulnerability assessments are recommended when new arms control treaties or agreements enter into force and when changes occur at a facility that could create new arms control obligations. These changes might include the acquisition of a new program, activity, or asset covered by treaty provisions.

When requested, DTIRP provides assessment assistance to facilities where DoD equities are located. DTIRP's role is to assemble and manage the assessment team and to direct assessment activities.

Purposes

The purpose of arms control security vulnerability assessments is ultimately to ensure that facilities are able to successfully meet the following two goals set by the United States for all on-site inspection activities:

- demonstrate treaty compliance; and to
- protect national security, proprietary, and other sensitive information from possible inadvertent disclosure.

Meeting these dual objectives can be a daunting task. Arms control inspectors will necessarily be allowed access to sensitive areas and information in order to collect the information needed to verify treaty compliance. This level of access to normally restricted areas, creates unique security



challenges for even the most robust facility security programs.

A key purpose of a vulnerability assessment is to identify and analyze inspectable areas. The types of inspection activities and items of inspection equipment that may be used in each area will also be determined. This information is essential for enabling the assessment team to accurately assess risks prior to recommending additional security countermeasures.

For security countermeasures to be appropriate and cost-effective, they need to be based on the following criteria:

- inherent value of the equity or information being protected;
- probability of the equity or information being observed and exploited; and the
- degree of harm expected to result in the event the equity or information is detected.

Personnel

To successfully complete the analytical tasks required during an arms control security vulnerability assessment, the assessment team will include individuals having expert knowledge of treaty provisions and DoD arms control policy

guidance. Facility personnel having expert knowledge of facility operations and processes will also be essential members of the team.

Assessment team members will have a range of specialized backgrounds. As needed, members will likely include countermeasures specialists, counterintelligence professionals, and individuals with expertise in information security, dual-use technologies, and in operations security. Team members are drawn from throughout the U.S. government and the arms control community. They will work with facility personnel to conduct assessment activities with the maximum efficiency and effectiveness.

Each team is tailored to the facility's unique arms control security challenges. Typically, vulnerability assessment teams consist of eight or more arms control treaty and security experts. However, the exact size and composition of the team depends on the size of the facility, the number of inspectable areas on site, and the types of technologies and operations located at the facility and in the surrounding area. Team size and composition also depend on the verification provisions of relevant treaties or agreements and the types of inspection activities that could occur.

Assessment Process

The assessment process is divided into five phases. The objectives and tasks conducted during each phase are described in the relevant subsections below.

Phase I: Coordination

The first phase of an arms control security vulnerability assessment begins when DTIRP receives a request for assistance. This request triggers a number of planning and preparation activities. These activities include gathering as much information as possible about the facility to be assessed and identifying the relevant arms control treaties and agreements.

The verification provisions of each applicable treaty will be reviewed to determine their potential impact on facility operations. In addition, the

necessary members of the assessment team will be selected, logistical requirements will be defined, and work will begin on developing the assessment plan.

To facilitate these efforts, the facility and its parent organization will be provided with a point of contact (POC) who will be responsible for coordinating assessment activities. The POC will be located in the Countermeasures Branch, Operations Support Division, On-Site Inspection Directorate at the Defense Threat Reduction Agency (DTRA). DTRA is DoD's executive agent for DTIRP.

The POC will begin interviewing key facility personnel and gathering background information about the facility's history. If any vulnerability assessments have been conducted in the past, a copy of the reports from these assessments should be sent to the POC. These reports will facilitate the process of preparing for and planning assessment activities.

Phase II: Open Source Data Search and Assessment Team Training

In the second phase of the assessment process, assessment team members will conduct a Web-based data search. They will collect as much information as possible about the facility from open sources and compile this information into a *Facility Profile Report*.

The *Facility Profile Report* will help team members to prepare for assessment tasks. Of particular interest will be information concerning the facility's operations, defense programs, personnel, financial status, and geographic location. Being aware of the open source information available is important because the inspection team will also have access to this information before they arrive on site.

When preparing to conduct inspection activities, representatives of the inspecting state party or international treaty implementation organization will develop an inspection plan. This plan will be based not only on the information provided by the United States in data declarations, if any, but also on the information available from open sources.

Phase III: Pre-Assessments

Pre-assessment activities may be conducted to determine whether a full-scale assessment is required. During a pre-assessment visit, team members will work with facility staff to identify critical assets, operations, and information that could, potentially, be at risk during an on-site inspection due to their nature or to their proximity to inspectable areas.

Pre-assessment visits are particularly useful when new treaties are being negotiated or are expected to enter into force in the near future. Pre-assessment visits are also useful when facilities are preparing an initial data declaration.

During pre-assessments, team members may determine that further assessment visits are *not* necessary. When this is the case, the assessment process will end at this point. However, when a full-scale assessment is justified, pre-assessment team members will work with facility personnel to plan the scope of full-scale assessment activities and to identify personnel requirements.

Phase IV: Full-Scale Assessments

The activities conducted during a full-scale assessment are tailored to the facility's specific arms control security concerns. These concerns may relate to possibilities for technology transfer, exposure to counterintelligence activities, or the facility's ability to maintain industrial, physical, and information security.

The assessment process itself consists primarily of collecting and analyzing information. Team members work with facility personnel to collect information about the facility's assets, operations, and existing security procedures. This information is collected by means such as briefings, personnel interviews, facility tours, and records reviews.

To maximize the assessment team's ability to cover multiple areas, team members usually break into subgroups during the day. In the evening, the groups meet together to collate, cross check, and analyze the information

collected. Team members also plan subsequent assessment tasks and begin developing a comprehensive picture of the facility's operations, personnel, and programs.

The accuracy of this picture depends very much on the quality and quantity of information provided to assessment team members by facility staff. The more accurate and detailed this information is, the more effective the assessment team will be in assessing and prioritizing risks, and in recommending appropriate and cost-effective security countermeasures.

Phase V: Reporting

At the end of on-site assessment activities, team members will provide a *Quicklook Assessment Report* to facility representatives. This report will summarize the team's observations, the facility's security concerns, and the team's recommended security countermeasures.

Subsequently, a detailed *Draft Assessment Report* will be prepared and forwarded to the agency or Service requesting the assessment. This report will include program-by-program and building-by-building assessments of potential vulnerabilities and location-specific recommended security countermeasures. When approved, the *Final Assessment Report* will be prepared. A copy will be sent to the facility Commander or Director.

Conclusion

This article has described how arms control security vulnerability assessments are conducted and how they can serve as a valuable tool for managing the security challenges associated with hosting on-site inspection activities.

For more information about arms control security-related topics, contact the DTIRP Outreach Program Coordinator at 1-800-419-2899, or by email at: dtirpoutreach@dtra.mil. Information and outreach materials are also available online on the DTIRP Website at: <http://dtirp.dtra.mil>. You may also contact your local Defense Security Service (DSS) Industrial Security Representative or your government sponsor.