

INTEGRATED SAFEGUARDS OPERATIONS SECURITY CHECKLISTS



U.S.-IAEA SAFEGUARDS AGREEMENT
U.S.-IAEA ADDITIONAL PROTOCOL

Product No.

608P



This pamphlet was prepared by the Defense Treaty Inspection Readiness Program (DTIRP) to increase **Readiness Through Awareness** throughout the Department of Defense (DoD) and defense-contractor community. Additional copies of this pamphlet as well as other information and materials on arms control security-related topics are available through the DTIRP Outreach Program.

July 2009

Prepared for:
DTIRP Outreach Program
Defense Threat Reduction Agency
8725 John J. Kingman Road, Stop 6201
Fort Belvoir, VA 22060-6201

From the DTIRP Outreach series: Product No. 608P

TABLE OF CONTENTS

Introduction.....	2
Checklists	4
Equity / Sensitive Information Identification	4
Susceptibility / Probability Determination.....	6
Threat Analysis	7
Vulnerability Analysis.....	8
Risk Assessment	9
Countermeasures Recommendations	9
Related Materials	10

INTRODUCTION

This pamphlet provides checklists to assist facility managers, security officers, and other arms control treaty implementers with adhering to the minimum standard items to be considered while conducting security vulnerability assessments (SVAs) of Department of Defense (DoD) interests located in proximity to sites, facilities, or activities eligible to be declared under integrated safeguards agreements. These agreements between the United States and the International Atomic Energy Agency (IAEA), are the U.S.-IAEA Safeguards Agreement (or Voluntary Offer) and the U.S.-IAEA Additional Protocol (AP).

Although no locations of direct national security significance will be declared or be subject to IAEA inspections, SVA's are required for DoD equities (facilities, programs, information, and activities) located at or near declarable activities. Eligible facilities primarily include Department of Energy (DOE) facilities, Nuclear Regulatory Commission (NRC) licensees, or private industry facilities declared via the Department of Commerce (DOC).

The checklists in this pamphlet are not intended to replace existing Component or Agency security procedures for conducting vulnerability assessments. However, arms control treaty compliance officers should carefully consider these checklists for each equity being assessed and should incorporate these checklists into existing processes when appropriate.

A separate checklist is provided for each of the following phases of the operations security (OPSEC) assessment process:

- Equity / Sensitive Information Identification
- Susceptibility / Probability Determination
- Threat Analysis
- Vulnerability Analysis
- Risk Assessment
- Countermeasures Recommendations

The equity / sensitive information identification phase focuses on identifying DoD programs and activities, as well as national security, proprietary, and other sensitive information located at potentially declarable sites. Once identified, the susceptibility of the DoD equity to on-site inspection activities and the probability of IAEA inspectors gaining access to the equity are determined. If IAEA inspectors could have access to the area, the potential threat posed by the inspection team and their equipment is analyzed.

Potential vulnerabilities are analyzed to determine whether existing protective measures would adequately prevent the inspection team from collecting sensitive information through observation, sampling and analysis, or other allowable activities. Once vulnerability is determined, a risk assessment is conducted. Assessing risk involves reviewing the level of access the inspection team may be permitted to sensitive information or areas, as well as the inspectors' capabilities and motivation to collect information about DoD equities.

Based on the risk assessment, countermeasures or managed access procedures may be recommended to ensure the continued protection of DoD equities during inspection activities. Whenever possible, recommended countermeasures should be transparent to the inspection team.

CHECKLISTS

EQUITY / SENSITIVE INFORMATION IDENTIFICATION

The first—and probably most difficult—phase of the assessment process is to collect the information needed to identify the security concerns potentially impacting DoD equities (facilities, programs, information, and activities) located in proximity to sites eligible to be declared under integrated safeguards agreements (the U.S.-IAEA Safeguards Agreement and the U.S.-IAEA Additional Protocol). This step is key to the remainder of the assessment process and adequate time should be taken to understand a facility's programs and to collect all necessary information.

The location of each activity and every aspect of each program—both sensitive and unclassified—need to be identified. Then a well-informed determination can be made about which programs and activities are sensitive. It is also important to evaluate whether any single or cumulative amount of unclassified information could indicate that a sensitive program or activity is present.

To identify sensitive information, it is more timely and cost-effective to follow a program or activity to each location rather than to inspect each structure or area on a facility. When a number of sensitive programs or activities are present, collocated activities (from different programs) and DOE inspectable areas can be noted. Plotting these program components on a site diagram may be useful for tracking activities.

- Determine the number of sensitive programs or activities.
- Identify the location of program activities and their subcomponents relative to declarable activities.
- Determine whether a program has proprietary information that must be protected.*
- Identify DoD equities collocated with declarable activities at the facility.
- Where DoD equities reside, determine whether a facility or building engages in declarable activities subject to inspection under integrated safeguards agreements.*

- Determine whether a facility or building houses national security or other sensitive equities.*
- Identify records, reports, plans, or materials located inside inspectable area relating to DoD equities.
- Identify observable, special, or unique equipment relating to DoD equities.
- Identify observable activities or operations indicative of DoD equities.
- Identify personnel whose presence or observable activities are related to—or are perceived to be related to—DoD equities.
- Identify unique or specialized materials or subcomponents relating to DoD equities.
- Identify unique or specialized safety or security procedures relating to DoD equities.
- Identify unique facility configurations or structures relating to DoD equities.
- Identify unique or specialized suppliers whose products or services relate to DoD equities.
- Identify solid, liquid, or gaseous waste products or by-products relating to DoD equities.
- Identify DoD activities collocated with or in close proximity to declarable facilities or items.
- List each identified item by category and priority on a worksheet, and classify findings, as necessary.

*Coordination with the DoD Treaty Office may facilitate determination.

SUSCEPTIBILITY / PROBABILITY DETERMINATION

Understanding the rights and obligations of IAEA inspectors, as well as inspection modalities, will assist in determining whether an inspector could have a right to access a location in proximity to sensitive information. Susceptibility and probability will need to be determined at each location where a declarable activity is present. Some level of probability for inspection activities exists at all declarable locations.

- For each DoD equity or sensitive indicator, determine the required inspector access for each collocated declarable item.
- Determine inspector proximity to the DoD equity during their access to a declarable item.
- Specify the probable inspection activity related to each inspectable item and collocated equity or sensitive indicator (observation, measurement, sampling, etc.).
- Determine whether the DoD equity has any signature of concern.
- Review the site's history with respect to activities of interest to the inspectors.

THREAT ANALYSIS

IAEA inspectors have significant technical expertise pertaining to the conduct of inspection and collection activities. It is important to assume that these inspectors will be capable of, and interested in, exploiting inspection activities against a DoD equity.*

- Determine the inspection team's capability for collecting information about DoD equities.

- Identify inspection equipment that could be used to collect information about declarable items.

- Determine whether inspection equipment could collect information about DoD equities.

*Coordination with the DoD Treaty Office may facilitate determination.

VULNERABILITY ANALYSIS

To determine vulnerability, it is necessary to overlay: 1) the susceptible areas' proximity to declarable activities; 2) the presence of the threat (the inspectors and their equipment); and 3) the sensitive equity or information. If susceptibility, threat, and sensitive information overlap, then a true vulnerability exists.

- Determine whether existing security classification guidance and physical security procedures adequately protect DoD equities from the data collection activities to be conducted by the inspection team.

- Determine whether sensitive indicators are visible or vulnerable due to their location.

- Determine whether DoD equities are vulnerable to visual observation.

- Determine whether DoD equities are vulnerable to sample analysis.

RISK ASSESSMENT

At each location it is necessary to determine whether inspection activities place DoD equities at risk. From the information developed during the threat and vulnerability phases, it is possible to determine risk. The level of risk will vary for each equity.

- Determine the level of risk to DoD equities based on threat and vulnerability.

COUNTERMEASURES RECOMMENDATIONS

Countermeasures are actions or techniques designed to diminish the inspectors' ability to collect information about critical DoD equities. To ensure that these measures are cost-effective, they should be based on assessed risks. Facility staff should also avoid applying any countermeasures that are likely to draw unwanted attention from the inspection team. The best countermeasures are transparent to the inspectors.

Appropriate countermeasures may include managed access techniques such as route planning and shrouding. For example, the route the inspectors take when entering, existing, and traveling inside a facility should be planned to avoid areas where indicators of critical information may be observed.

RELATED MATERIALS

To order copies of the products listed below, contact the DTIRP Outreach Program Coordinator by phone at 1-800-419-2899 or by email at dtirpoutreach@dtra.mil. Visit the DTIRP Website at <http://dtirp.dtra.mil> to view, print, or order DTIRP products.

Pamphlets

Integrated Safeguards: U.S.-IAEA Safeguards Agreement and U.S.-IAEA Additional Protocol (612P)

Complementary and Managed Access under the U.S.-IAEA Additional Protocol (613P)

Understanding the U.S.-IAEA Additional Protocol National Security Exclusion (**NSE**) (**614P**)

Arms Control Agreements Synopses (408P)

The Arms Control Inspector (406P)

Guide to Arms Control Policy and Implementation Organizations (411P)

Arms Control Abbreviations and Acronyms Guide (946P)

DTIRP Arms Control Outreach Catalog (907P)

Videos on CD

Facility Protection Through Shrouding (908W)

Verification Provisions—Point and Counterpoint (936W)

The Technical Equipment Inspection (TEI) Process (950W)

Automated CDs

The Arms Control OPSEC Process (930C)

Searchable CDs

Arms Control Treaties—A Reference Guide (407C)

DTIRP Outreach Products (942C)

Brochures

Why TEI? (954T)

NOTES

NOTES



Distributed by:

DTIRP Outreach Program
Defense Threat Reduction Agency
8725 John J. Kingman Road, Stop 6201
Fort Belvoir, VA 22060-6201
1-800-419-2899
dtirpoutreach@dtra.mil
<http://dtirp.dtra.mil>

Product No.

608P