

Arms Control **SECURITY**

Challenges and Countermeasures



**Order No.
934P**



October 2006

This pamphlet is part of a series of educational outreach products promoting arms control security awareness. The pamphlet was prepared for the Defense Treaty Inspection Readiness Program (DTIRP) to increase **Readiness Through Awareness** within the Department of Defense (DoD) and defense contractor community. Additional copies of this, and other educational materials on arms control treaty implementation and security-related topics, are available through the DTIRP Outreach Program Coordinator and on the DTIRP Website at: <http://dtirp.dtra.mil>.

October 2006

Prepared for:
DTIRP Outreach Program
Defense Threat Reduction Agency
8725 John J. Kingman Road, Stop 6201
Fort Belvoir, VA 22060-6201
1.800.419.2899
Email: dtirpoutreach@dtra.mil
Web: <http://dtirp.dtra.mil>

From the DTIRP Outreach series: Order No. 934P

TABLE OF CONTENTS

BACKGROUND	2
CROSS-TREATY SYNERGY	3
ARMS CONTROL SECURITY	6
Identify Critical Information and Its Indicators	10
Analyze the Threat	14
Analyze Vulnerability	16
Assess Risk	16
Develop and Implement Security Countermeasures	17
CHECKLISTS	19
Checklist: Identify Critical Information and Its Indicators	19
Checklist: Analyze the Threat	21
Checklist: Analyze Vulnerability	22
Checklist: Assess Risk	23
Checklist: Develop and Implement Security Countermeasures	24
CONCLUSION	25
LIST OF ABBREVIATIONS	26
RELATED MATERIALS	27



BACKGROUND

Arms control treaties and agreements may contain provisions allowing inspectors from other States Parties to verify compliance by conducting on-site inspection activities and observation mission flights. Although these activities benefit the United States by promoting mutual trust and confidence, they also create unique security challenges at the sites and facilities affected.

Department of Defense (DoD) and defense contractor facilities have been subject to arms control treaty compliance verification activities since 1987, when Presidents Reagan and Gorbachev signed the Intermediate-Range Nuclear Forces (INF) Treaty. Since that time, DoD commanders, program managers, and other facility staff members have had to increase their awareness of the appropriate arms control security procedures for demonstrating treaty compliance while also protecting critical information from inadvertent disclosure.

Given the number of arms control treaties and agreements in force, it is also important to consider potential cross-treaty synergy risks when developing an arms control security plan. Cross-treaty synergy is the idea that an adversary or economic competitor could attempt to take advantage of multiple treaties' verification regimes to collect information that could not, otherwise, be obtained. Under these circumstances, critical information at facilities that are subject to multiple verification regimes could be at greater risk.

This pamphlet begins by outlining some potential scenarios under which cross-treaty synergy could, potentially, succeed. It also describes the processes for assessing arms control security risks and developing appropriate and cost-effective security countermeasures.

CROSS-TREATY SYNERGY

It is understood throughout the intelligence community that the synergy of information gathered from multiple sources provides greater insight than information collected from a single source (see Figure 1). When preparing for on-site inspection activities, it is essential to assume that the inspection team will be aware of all open source information relevant to your facility. This information can be gathered from the Internet, from satellites, and from human and other sources. Whether your facility is subject to the verification regimes of one or multiple arms control treaties, you should assume that foreign governments and international treaty-implementation organizations will have also briefed the inspection team on all available information about your facility.

An example of the potential use of cross-treaty synergy occurred during the NATO mission in Kosovo. During an approximate 10-day period, it appeared that Russia and Belarus were attempting to couple arms control treaty compliance verification activities with other intelligence-gathering efforts to gain information about NATO operations at military bases located in Italy, Germany, Hungary, the United Kingdom, Albania, and Macedonia. By using information obtained from the media, as well as from official NATO and other national sources, these two countries seemed to be attempting to conduct on-site inspection activities at NATO facilities for the purpose of confirming open source information pertaining to NATO's order of battle, force strength, and activity schedules.



Figure 1: Use of treaty verification measures to supplement other sources of information

Due to the unique nature of the security challenges associated with implementing arms control treaties and agreements, it is important to understand *whether* and *how* multiple verification regimes could, potentially, magnify these challenges at your facility. Specifically, it is important to determine *how* an adversary or economic competitor could attempt to use the verification provisions of one or more treaties (see Figure 2) to collect information about critical assets, equities, programs, operations, and activities that could not, otherwise, be obtained.

When evaluating the potential impact of one or more arms control treaties or agreements on your facility’s security, and when developing an arms control security plan, it is important to consider the answers to the following questions:

- Q:** Could multiple on-site inspections and/or observation mission flights be conducted at, or over, my facility for the purpose of collecting information about critical assets, equities, programs, operations, or activities?
- Q:** Could imagery collected during a Treaty on Open Skies observation mission flight be used to prepare an inspection team to conduct a challenge inspection under the CWC?
- Q:** Could multiple inspections and/or observation mission flights place critical information at increased risk?

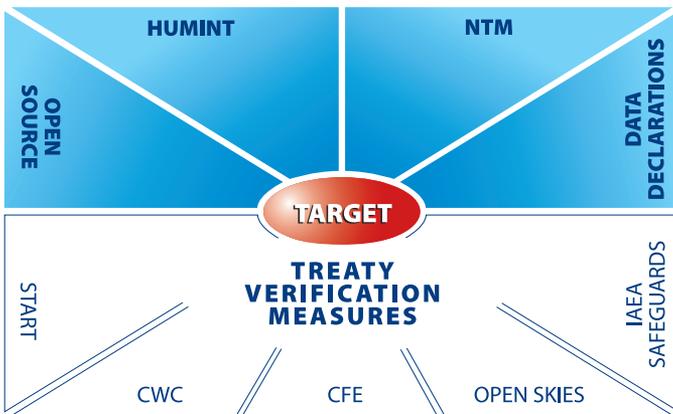


Figure 2: Use of multiple treaty verification regimes to collect information about a single target

To answer these questions effectively, it is important to consider the difficulties a State Party would be required to overcome before being capable of implementing a cross-treaty synergy strategy. To collect specific information using one or more arms control treaty compliance verification regimes, the following conditions would need to be met:

- the State Party would need to know that the desired information was vulnerable during the special types of access afforded by the compliance verification activities conducted at a particular site or facility;
- there would need to be an effective “overlap” of compliance verification activities allowing the State Party to influence these activities;
- the State Party would need to be able to affect the activities of certain members of the inspection team—this would be particularly difficult under agreements implemented by international organizations such as the Organization for the Prohibition of Chemical Weapons (OPCW) or the International Atomic Energy Agency (IAEA), which employ and send international inspection teams; and
- the State Party would need to assume that the security countermeasures and national escorts deployed by the Inspected State Party would be unable to sufficiently protect the desired information.

Although not impossible, meeting all of these criteria would be extremely difficult for any State Party.



ARMS CONTROL SECURITY

The compliance verification regimes of arms control treaties and agreements are intentionally designed to allow international inspection teams to penetrate several layers of security measures facilities normally use to protect critical information (see Figure 3). The degree of penetration depends on the specific provisions of a treaty and its verification regime.

The following are some examples of specific treaty provisions that define and limit the areas of a facility that may be inspected:

- The Strategic Arms Reduction Treaty (START) includes specific size criteria for access to specific areas. These criteria are linked to the smallest types of equipment declared to be present at the inspection site. The smallest length and diameter of a single item of inspection under START is 6.3 x 1.88 meters for the Minuteman II/III missiles.
- The provisions of the Treaty on Conventional Armed Forces in Europe (CFE) limit the inspectors' access to areas having an entrance larger than 2 meters.
- Under the CWC, inspectors have the right to request access to buildings and structures and to conduct activities such as taking samples, analyzing those samples, reviewing records, and conducting interviews with facility personnel. However, all of these activities are subject to negotiation.

The rights provided under these and other arms control treaties and agreements may allow international inspection teams to request access to information and areas at U.S. facilities where traditional security measures may not be sufficient to protect critical information. In these unique circumstances, DTIRP can help facilities develop appropriate and cost-effective security countermeasures that focus on the unique security risks posed by the presence of an international inspection team and which can be applied as needed. DTIRP can also help facilities prepare an effective arms control security readiness plan and manage inspection-related activities.

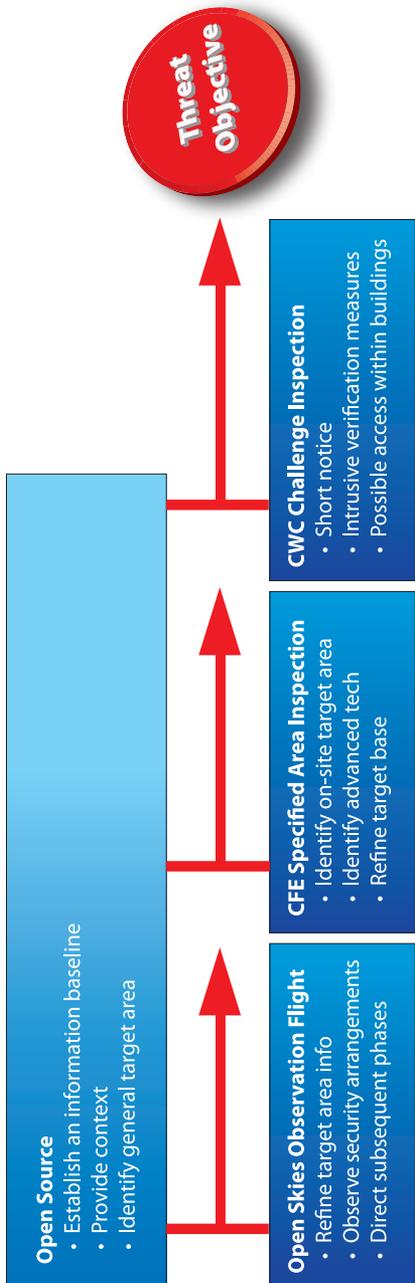


Figure 3: Indicators of Critical Information



THE ELEMENTS OF ARMS CONTROL SECURITY

The elements of the arms control security process are listed below in Box 1. These elements are similar to those of traditional operations security (OPSEC) processes, but the arms control security process involves making a determination about a facility's potential susceptibility to the verification provisions of an arms control treaty or agreement. It also involves assessing the likelihood, or *probability*, of verification activities actually occurring at your facility and whether such activities could place critical information at risk.

The process begins with identifying critical information and any unprotected indicators of that information located at, or in proximity to, your facility. The threat posed by the inspectors' capabilities and potential motivations for collecting information needs to be analyzed. In addition, potential vulnerabilities need to be analyzed to identify *true* vulnerabilities. True vulnerabilities exist when there is a direct link between a discernable indicator and a real collection threat.

ELEMENTS OF ARMS CONTROL SECURITY

- **Identify critical information and its indicators**
- **Analyze the threat**
 - **Determine susceptibility to treaty provisions**
- **Analyze vulnerability**
- **Assess the risk of compromise**
 - **Assess the probability of inspection activities occurring**
- **Develop and implement security countermeasures**

Box 1

A risk assessment is conducted to determine the likelihood, or probability, of a member of an inspection team collecting critical information during on-site inspection activities. Based on all of these analyses and assessments, it is possible to develop appropriate and cost-effective security countermeasures that can be implemented as needed to effectively manage arms control security risks.

DTIRP is able to assist facilities with conducting an arms control security assessment and with preparing for and managing on-site inspection activities. In accordance with a facility's unique arms control security needs, DTIRP can provide arms control treaty and security experts to support facility staff. These experts have a thorough understanding of DoD and Service guidance and understand how treaty provisions can be used to either grant or limit the inspection team's access to sensitive areas and information.

The ultimate goal of all arms control security activities is to prepare treaty implementers to be able to *demonstrate treaty compliance while also protecting national security, proprietary, and other critical information* from inadvertent disclosure during arms control treaty compliance verification activities.

IDENTIFY CRITICAL INFORMATION AND ITS INDICATORS

Identifying critical information and any observable indicators of critical information located throughout, or in proximity to, your facility is of key importance to the arms control security process. As shown in Figure 4, there are many types of indicators of critical information. These indicators may include unclassified or unprotected components, elements, or processes associated with critical assets, equities, programs, operations, or activities.

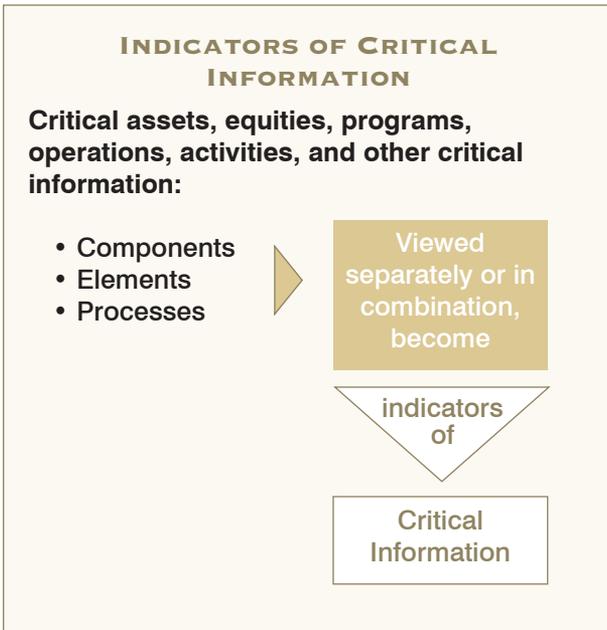


Figure 4: Indicators of Critical Information

WHAT IS CRITICAL INFORMATION?

Critical information is information that, if compromised, is intrinsically harmful and would likely undermine the objectives of a critical program, in whole or in part, or provide an economic competitor or adversary with an unacceptable advantage.

TYPES OF INDICATORS

Indicators of critical information are data or information that may be collected from open sources or from observable activities. If collected by unauthorized personnel, such information could lead an individual to reach conclusions about, interrupt, or derive estimates about the intentions, capabilities, or activities associated with critical assets, programs, or operations. These indicators can be *anything* that, when detected, either separately or in combination with other indicators or information, has the potential to reveal information about assets, equities, programs, operations, or activities that should be protected (see Figures 4, 5 and 6).

Figure 5 lists a number of the common types of potential indicators of critical information.

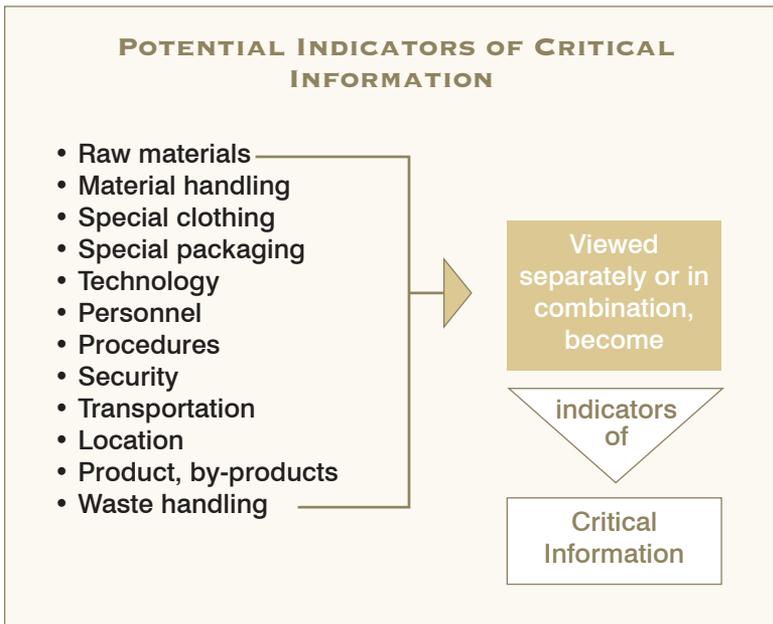


Figure 5: Potential Indicators of Critical Information



A brief description of each of these potential indicators is provided to illustrate the types of indicators that may exist at your facility. Understanding how to identify these indicators is very important for maintaining effective security during on-site inspection activities.

Raw Materials

Raw materials can be anything used in a production process or as part of an operation or activity. These materials are usually stored on site. If they can be observed and understood to be part of a critical program or activity, they may need to be protected during on-site inspection activities or observation overflights.

Material Handling

If special procedures are required for handling materials used in a critical program or activity, these procedures could serve as an indicator of critical information.

Special Clothing

Special clothing and personal protection equipment worn as part of a critical program or activity could be indicators of critical information.

Special Packaging

Special packaging used for raw materials or products could be an indicator of critical information. It is important to identify any unique packaging associated with the materials and products used in critical programs and activities.

Technology

The use of special tools, technologies, or equipment could provide evidence of the existence of a critical program or activity. In addition, maintenance or replacement parts for such tools, technologies, or equipment could also be indicators of critical information.

Personnel

If some personnel working on critical programs or activities appear distinctly different from other facility staff, they could serve as indicators of critical information, if observed.

Procedures

Unusual procedures or working hours that are noticeably different from other facility operations could be interpreted as indicators of a critical program or activity.

Security

Distinctive badging or special security practices could serve as indicators of critical programs or activities. Facilities may apply higher levels of security in certain areas, such as those used for research and development and other sensitive operations. *It will be important to identify any distinctive security practices that may be observable in inspectable areas.*

Transportation

If sensitive programs or activities rely on special types of transportation for shipping equipment, raw materials, or products, evidence of such transportation systems could be indicators of critical information. These transportation systems could include aircraft, runways, train tracks, or special vehicles. It will be important to determine whether any evidence of these systems is present in the inspectable areas or is observable elsewhere on the facility or in the surrounding area.

Location

The location of sensitive programs and activities can also serve as an indicator of critical information. If a program or activity is located deep within a facility, or in a remote area, this fact alone could be an indicator of the sensitive aspects of a critical program or activity.



Product, By-Products

The final product, or by-products, of a critical program or activity could reveal information about the program or activity. It will be important to consider whether such products and by-products could be observed during on-site inspection activities and whether they could serve as indicators of critical information.

Waste Handling

Waste handling and treatment areas are repositories for by-products from past and present programs and activities. It will be important to determine whether certain waste by-products, or the procedures for handling these waste by-products, could serve as indicators of critical information.

ANALYZE THE THREAT

Analyzing the threat posed by the presence of an international inspection team involves gaining an understanding of each inspector's potential interest and ability to collect, process, analyze, and utilize information. This requires learning as much as possible about an adversary or economic competitor and the strategies available for targeting critical programs and activities at your facility.

It is essential to tailor your analysis of the threat to the actual programs and activities occurring at your facility. To gain an understanding of an inspector's overall intentions, it will be helpful to answer questions such as:

- Q:** Why would an adversary or economic competitor want information about this program or activity?
- Q:** What are the adversary's goals?

It will then be possible to develop a description of the collection threat posed by inspectors tasked with collecting intelligence information during on-site inspection activities. These capabilities must also be evaluated in relation to the inspection provisions of the specific treaty involved.

DETERMINE SUSCEPTIBILITY

To determine whether your facility is susceptible to the verification provisions of a particular arms control treaty or agreement, it is necessary to have a thorough understanding of the treaty's objectives and verification regime. This knowledge will enable you to identify your facility's inspectable areas as well as the types of tools and equipment available to the inspection team. These tools may include access, observation, measuring, photography, sampling and analysis, record and document reviews, and personnel interviews.

Within inspectable areas, it is important to determine whether the inspectors would be able to detect critical information or its indicators by using permitted equipment. For example, it could be important to determine whether the inspectors might be able to detect chemicals or compounds from previous activities if they were to analyze a soil or dust sample.

In locations where shared activities are present, it is essential to identify and protect the indicators of critical information. *Indicators and locations outside inspectable areas are not considered to be susceptible unless they can be observed by the inspection team.*

DOES THIS ARMS CONTROL TREATY AFFECT MY FACILITY?

To determine whether a particular arms control treaty could affect your facility, it is useful to answer the following questions:

- Q:** Does my facility possess or engage in activities that make it subject to the treaty's verification provisions?
- Q:** Does my facility have the appearance of being subject to the treaty?

If the answer to either of these questions is "yes," then it is recommended that facility staff conduct an arms control security vulnerability assessment.



ANALYZE VULNERABILITY

To analyze your facility's vulnerabilities, it is important to consider the following three elements of the arms control security process simultaneously. These are:

- 1) your facility's critical information and its indicators;
- 2) the threat posed by the inspection team; and
- 3) your facility's inspectable areas.

Any special skills, such as intelligence or technological expertise, possessed by members of the inspection team need to be considered as well as the tools and equipment that may be used inside inspectable areas.

By analyzing how tools such as access, observation, photography, sampling and analysis, record reviews, and personnel interviews may be used inside each area to be inspected, it will be possible to eliminate *hypothetical* risks and to identify *actual vulnerabilities*. *True vulnerabilities exist when there is a direct link between a discernable indicator and a real collection threat.*

ASSESS RISK

An assessment should be made of the likelihood, or *probability*, of the inspection team actually collecting information about critical assets, equities, programs, operations, or activities. This assessment involves comparing the intelligence collection objectives and capabilities of the inspection team with the vulnerabilities and indicators of critical information that have been identified.

A risk assessment also involves examining any mitigating circumstances, such as time, that may reduce or eliminate risk. For example, if an indicator cannot be detected or observed by the inspection team during on-site inspection activities, it will not be vulnerable and will not require protection. However, even though all members of the inspection team will, in most cases, abide by treaty protocols, *observable activities or operations that could serve as indicators of critical information needs to be protected.*

DEVELOP AND IMPLEMENT SECURITY COUNTERMEASURES

Once you have determined which indicators and information need to be protected during on-site inspections or observation mission flights, it is time to develop and implement appropriate and cost-effective security countermeasures. Important decisions will need to be made about what *types* of security countermeasures should be selected and *when* each countermeasure should be applied. *Remember: if a countermeasure is more expensive to implement than the value of the information being protected, it returns no benefit.*

If on-site inspection activities are not likely to occur, or if they are expected to occur very rarely, it may be prudent to develop countermeasures that can be implemented quickly when needed. Keep in mind that the time available to prepare a site for on-site inspection activities or for observation mission flights will be short.

The best security countermeasures are transparent to the inspection team and all countermeasures should not only protect information but also allow the inspection team to determine that there are no compliance concerns at your facility. Most arms control treaties and agreements specifically obligate the Inspected State Party to demonstrate that protective measures are not masking noncompliance. *Remember, a countermeasure that creates ambiguities could invite unwelcome attention and questions from the inspection team.*

TYPES OF SECURITY COUNTERMEASURES

Appropriate types of security countermeasures range from simple procedural changes to perception management, intelligence countermeasures, and other techniques to diminish the inspection team's ability to collect information. Appropriate countermeasures may include the use of tactics such as diversion, concealment, shrouding, and camouflage to disrupt or prevent the inspection team from accessing or interpreting indicators of critical information. For example, preplanned routes through your facility or through a particular building may be developed and suggested to the inspection team. By following these preferred routes, it may be possible to avoid sensitive areas, programs, and activities.



Other types of security countermeasure include counteranalysis measures and action controls. Action controls either eliminate or change the “who,” “what,” “where,” or “how” of an activity that could otherwise serve as an indicator of critical information. For example, a test, process, or operation could be rescheduled to a time when the inspection team would not be present. Counteranalysis measures attempt to prevent the interpretation of indicators of critical information by presenting an observable condition or situation that leads the inspection team away from the indicator.

CHECKLISTS

The checklists provided in this pamphlet are designed to help you conduct a self-assessment of your facility's readiness to meet the arms control security challenges posed by on-site inspections and observation mission flights. A separate checklist is provided for each element of the arms control security process (see Box 1 on page 8).

CHECKLIST: IDENTIFY CRITICAL INFORMATION AND ITS INDICATORS

Accurately identifying critical information and its indicators is of key importance to managing your facility's security during on-site inspections and observation mission flights. To complete this task, it is recommended that facility staff use the checklist provided below and follow each critical asset, equity, program, operation, or activity throughout the facility to collect information about each location that either supports, or is affected by, these programs.

This method of following critical programs or activities throughout a facility is generally preferred because it has been found to be more efficient and effective than inspecting individual structures and areas.

If there are a number of critical programs and activities at your facility, it will be essential to identify any locations inside inspectable areas where these activities are collocated. Plotting the locations of critical programs and their components on a site diagram is very helpful.

- Identify all assets, equities, programs, operations, and activities on the facility.
- Identify the locations of all assets, equities, programs, operations, and activities and their subcomponents.
- Determine whether there is critical information associated with an asset, equity, program, operation, or activity that needs to be protected.
- Identify critical programs and activities collocated with declarable or potentially inspectable areas and activities.



- Where critical equities, programs, and activities reside, determine whether a facility or building in proximity to that equity, program, or activity engages in activities subject to on-site inspection activities under an arms control treaty or agreement.
- Identify records, reports, plans, and materials located inside the inspectable area(s) relating to critical assets, programs, or activities.
- Identify observable, special, or unique equipment relating to critical assets, programs, or activities.
- Identify observable activities or operations indicative of critical assets, programs, or activities.
- Identify personnel whose presence or observable activities are related to—or may be perceived to be related to—critical assets, programs, or activities.
- Identify unique or specialized materials and subcomponents relating to critical assets, programs, or activities.
- Identify unique or specialized safety or security procedures relating to critical assets, programs, or activities.
- Identify unique facility configurations or structures relating to critical assets, programs, or activities.
- Identify unique or specialized suppliers whose products or services are related to critical assets, programs, or activities.
- Identify solid, liquid, or gaseous waste products or by-products relating to critical assets, programs, or activities.
- Identify any critical assets, equities, programs, operations, and activities or any components or indicators of critical information that are collocated with, or in close proximity to, inspectable areas.
- On a worksheet, list by category and level of classification each asset, equity, program, operation, activity, component and indicator identified.

CHECKLIST: ANALYZE THE THREAT

The arms control security threat to be analyzed in this context is the threat posed by the on-site presence of individual members of an inspection team. Arms control treaty inspectors have a significant amount of technological expertise and it should be assumed that they are capable of exploiting opportunities to collect information. It will be important to gain a thorough understanding of each inspector's potential interests and abilities to collect, process, analyze, and utilize information. Part of this analysis will be to determine whether critical information and its indicators may or may not be susceptible to specific on-site inspection activities.

- Analyze each inspector's capabilities for collecting information about critical assets and activities.
- Identify each item of equipment the inspection team may use during on-site inspection activities.
- Analyze each item of inspection equipment to determine whether it could be used to collect critical information either directly or indirectly by collecting information about the indicators of critical assets or activities.
- Identify each inspector's nationality and any national programs that are similar to critical assets or activities.
- Identify each inspector's potential objectives for collecting information about critical assets or activities.
- Determine what level of access the inspectors are likely to be granted to each area where critical assets, activities, or the indicators of critical information are located or can be observed.
- Identify the types of inspection activities (access, observation, measurement, photography, sampling and analysis, record and document reviews, personnel interviews, etc.) that are likely to be conducted inside each inspectable area collocated with critical assets, activities, or the indicators of critical information.
- Determine whether critical assets or activities located in non-inspectable areas have signatures similar to inspectable items.



CHECKLIST: ANALYZE VULNERABILITY

To analyze your facility's vulnerabilities, it is important to simultaneously consider your critical information and its indicators, the threat posed by the inspection team, and your facility's inspectable areas. This analysis will help you to eliminate hypothetical risks and to identify actual vulnerabilities. True vulnerabilities exist when there is a *direct link between a discernable indicator and a real collection threat*.

- Determine whether security classification guidance and physical security procedures are adequate for protecting critical assets, programs, and operations during on-site inspection activities.
- Determine whether indicators of critical information are visible or vulnerable due to their location.
- Determine whether unclassified components or elements of critical assets, programs, and activities are vulnerable to visual observation.
- Determine whether unclassified components or elements of critical assets, programs, and activities are vulnerable to sampling analysis.

CHECKLIST: ASSESS RISK

A risk assessment involves determining the likelihood, or probably, of the inspection team actually collecting information about critical assets, equities, programs, operations, or activities. This assessment involves comparing the intelligence collection objectives and capabilities of the inspection team with the vulnerabilities and indicators of critical information that have been identified. If critical information or indicators are observable or can be revealed during on-site inspection activities, the level of risk is high and protective measures will be necessary.

- Assess the probability of inspection activities occurring at your facility or within proximity to critical assets, programs, or activities or indicators of critical information.
- Assess the likelihood of inspectors gaining access to areas where critical assets, programs, activities or indicators of critical information are located.
- Assess whether the inspection team would be capable of collecting information about critical assets, programs, and activities without having physical access to them (i.e., through the use of inspection equipment or by observing indicators of critical information).
- Assess individual inspector's potential motivations (political, economic exploitation, etc.)—including national will—for collecting information about critical assets, programs, or activities.
- Review your facility's history to identify past activities that may be of interest to the inspection team.



CHECKLIST: DEVELOP AND IMPLEMENT SECURITY COUNTERMEASURES

Security countermeasures should be cost-effective and be based on the assessed level of risk. Appropriate countermeasures include action controls or simple procedural changes that alter or eliminate the “who,” “what,” “where,” or “how” of an activity that could otherwise serve as an indicator of critical information.

Security countermeasures may also include diversion, concealment, shrouding, and camouflage measures that disrupt or prevent the inspectors from gaining access to, or collecting information about, critical assets, programs, and activities. In addition, counteranalysis measures can be used to prevent the inspectors from interpreting critical information by presenting an observable condition or situation that diverts their attention.

- Determine the effectiveness of countermeasures.
- Determine the usefulness of action controls (altering or eliminating the “who,” “what,” “where,” or “how” of critical information or indicators).
- Determine the value of counteranalysis measures (diversion, concealment, shrouding, and camouflage).
- Determine whether selected countermeasures are transparent to the inspectors.
- Determine whether managed access procedures can be used.
- Assess all selected countermeasures to ensure they do not create additional vulnerabilities.
- Evaluate all selected countermeasures to ensure they are treaty-compliant and cost-effective.

CONCLUSION

The arms control security process described in this pamphlet is designed to help facilities identify and effectively address the security challenges associated with implementing arms control treaties and agreements. Arms control treaty compliance verification regimes and the concept of cross-treaty synergy suggest that States Parties to multiple arms control treaties and agreements could, conceivably, attempt to manipulate these regimes to maximize their ability to collect sensitive information. A related arms control security concern is whether the possibility of such an attempt could increase a facility's risk of inadvertently disclosing national security, proprietary, or other critical information during on-site inspection activities.

For more information about how to ensure your facility's readiness from an arms control security standpoint, or to request assistance with conducting a vulnerability assessment or hosting on-site inspection activities, contact the DTIRP Outreach Program Coordinator at 1-800-419-2899, or send an email to dtirpoutreach@dtra.mil. You may also request assistance through your local Defense Security Service (DSS) Industrial Security Representative or from your government sponsor.

Additional arms control security information can be viewed and downloaded from the DTIRP Website at: <http://dtirp.dtra.mil>.



ABBREVIATIONS

CFE	Treaty on Conventional Armed Forces in Europe
CWC	Chemical Weapons Convention
DoD	Department of Defense
DSS	Defense Security Service
DTIRP	Defense Treaty Inspection Readiness Program
DTRA	Defense Threat Reduction Agency
IAEA	International Atomic Energy Agency
INF	Intermediate-Range Nuclear Forces Treaty
NATO	North Atlantic Treaty Organization
Open Skies	Treaty on Open Skies
START	Strategic Arms Reduction Treaty
TEI	Technical Equipment Inspection

RELATED MATERIALS

Videos on Windows-Compatible CD

Site Vulnerability Assessments (951W)
Security Countermeasures: Selection and Application (952W)
Inspection and Building Preparation (953W)
Verification Provisions—Point and Counterpoint (936W)
The Technical Equipment Inspection (TEI) Process (950W)
Facility Protection through Shrouding (908W)

Automated CDs

The Arms Control OPSEC Process (930C)

Searchable CDs

Arms Control Treaties (407C)
DTIRP Outreach Products on CD (942C)

Pamphlets

Arms Control Agreements Synopses (408P)
DTIRP Arms Control Outreach Catalog (907P)

Brochures

Why TEI? (954T)



NOTES

Order No. 934P



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

Email: dtirpoutreach@dtra.mil

Web: <http://dtirp.dtra.mil>

