

# **The Functional Requirements and Design Basis for Information Barriers**

**The Joint United States DOE-DOD Information Barrier  
Working Group**

**May 1999**

## DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY  
*operated by*  
BATTELLE  
*for the*  
UNITED STATES DEPARTMENT OF ENERGY  
*under Contract DE-ACO6-76RL01830*

Printed in the United States of America

Available to DOE and DOE contractors from the  
Office of Scientific and Technical Information,  
P.O. Box 62, Oak Ridge, TN 37831-0062;  
ph: (865) 576-8401  
fax: (865) 576-5728  
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,  
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161  
ph: (800) 553-6847  
fax: (703) 605-6900  
email: orders@ntis.fedworld.gov  
online ordering: <http://www.ntis.gov/ordering.htm>

# The Function Requirements and Design Basis for Information Barriers

## Executive Summary

The Departments of Defense and Energy jointly established the Information Barrier (IB) Working Group (IBWG) in late calendar year 1998 to devise optimal approaches to protecting classified nuclear weapons design information when utilizing radiation signature monitoring methods. The current focus of these activities is on potential US-Russian bilateral and trilateral agreements. It is important to note that at this writing the state of progress in the development of Trilateral Agreement monitoring equipment is well-advanced compared to the other two regimes, in anticipation of a mid-June 1999 demonstration to the IAEA and Russian Federation.[1] Information barriers may be needed for other agreements such as the Plutonium Production Reactor Agreement (PPRA), and the Processing, Packaging, and Inserts Agreement (PIIA).

This report summarizes the results of a workshop held at Sandia National Laboratory in Albuquerque, New Mexico during the period of February 2-4, 1999. This IBWG workshop was convened to establish the functional requirements associated with warhead radiation signature information barriers, to identify the major design elements of any such system or approach, and to identify a design basis for each of these major elements. Such information forms the general design basis to be used in designing, fabricating, and evaluating the complete integrated systems developed for specific purposes.

The fundamental functional requirements for the information barrier portion of an integrated radiation signature-information barrier inspection system are twofold:

1. The host must be assured that his classified warhead design information is protected from disclosure to the monitoring party, and
2. The monitoring party must be confident that the integrated inspection system measures, processes, and presents the radiation signature based measurement conclusion in an accurate and reproducible manner.

The requirement to protect host country classified warhead design information is fundamental and admits no tradeoff versus the confidence provided to the monitoring party in the accuracy and reproducibility of the measurements. This principle shaped the deliberations of the IBWG. The IBWG was able to enumerate ten critical design elements that define radiation signature information barriers. It also identified the design basis for these critical elements. The critical elements in the design of radiation signature information barriers are listed below and the design basis for each is summarized.

- **Supplier of the Integrated System.** With the primary functional requirement for the use of an integrated radiation signature measurement and information barrier system

being the absolute protection of host country classified warhead design information, determination of who supplies the equipment becomes the primary design issue. The Information Barrier Working Group concludes that the best approach to assuring the protection this information is that of the host country supplying the equipment. For the purpose of assessing information barriers, "supply" is associated with last sole possession, but not necessarily design or fabrication.

It is conceivable that some radiation inspection equipment may need to be utilized under what is referred to as the "mixed" approach. Under some inspection situations, the monitoring party could show up with its own radiation measurement devices, and these could be examined in their presence by the host country.

- **Central Processing Unit (CPU).** The recommended approach to selecting an overall system CPU or a set of processors sequenced in the classified data stream is that of dedicated, trusted processor architecture. The concept of a trusted processor is a hardware and software architecture that is dedicated to the specific processing task(s), having extraneous functionality minimized or eliminated, and is therefore more readily inspectable. Commercially available single-board computers are good platforms from which to design the trusted processor for warhead components and materials monitoring applications
- **Non-CPU Equipment.** The design considerations associated with the CPU are also relevant to non-CPU elements such as the detector subsystem, and the detector signal pulse-height or multi-channel analyzer (MCA) subsystem. The IBWG is in general agreement that commercially fabricated and procured detector subsystems, such as a high-purity germanium (HPGe) detector with an integrated analog pulse preamplifier and liquid nitrogen dewar, are inspectable. The inspectability of additional analog electronics and multi-channel analyzers needs to be evaluated on a case-by-case basis.
- **Procedural issues.** The procedural problem that must be addressed is how to keep a monitoring party from deducing sensitive information about the fissile material being examined simply as a result of the conduct of the inspection itself, rather than from the data collected. This need must again be assessed on a case-by-case basis. A particular problem is that detector placement and utilization. The guidance in this case is that the instrument should be able to autonomously determine and use the optimum counting time, geometry, etc., with the details of this process concealed by the IB.
- **TEMPEST/Electronic Emanation Considerations.** It is important under the condition of host-supplied inspection equipment that the host is assured that there are no electronic emanations from the measurement system that the monitoring party can record. Likewise, the monitoring party must have a high degree of confidence that the host cannot somehow control or adversely affect the proper operation of the inspection system during an actual measurement using radio control. The IBWG considers that conventional operational-security procedures, when combined with standard good design practice in minimizing electronic emanations, are sufficient to effect the necessary high degree of security required of the integrated system. The use of

dedicated trusted processor designs with completely understood control software, combined with a general approach of complete transparency in any integrated inspection system design, help assure the monitoring party that the host cannot illicitly control or affect inspection measurements. TEMPEST-level protection would offer the highest level of protection against surreptitious radio control of the measurement system, however.

- **Optimal Location of Barriers(s).** In the circumstance where there is little measured data that is not classified, such as that associated with radiation emanations from warhead items, some additional security may be afforded through the use of several intermediate barriers. While a layered data security approach is appealing, it is difficult to conceive of filters which could be effective in completely alleviating data security concerns for these types of inspection systems used for these purposes. At the same time, employing intermediate filters can be detrimental to checking system functionality. If intermediate barriers can be employed without compromising functionality assurances, then it is desirable to do so. Ultimately, it is at the system level that information security (including system use procedures) must be assessed, however.
- **Software, Firmware, and CPU Operating Systems.** Just as the data processing hardware must be completely inspectable, so too must the associated computer codes. The complete inspectability of the data processing hardware and software is critical to the trusted processor design concept. This necessitates that the amount of code be limited and that there be no extraneous code. It also suggests that more complex high-level software operating systems not be utilized. It is likely to require that system software modules be authenticated using hash function or other algorithmic based code-checking methods.
- **Storage, Authentication, and Disposition of Data and Data Media.** Unclassified attribute based inspection systems hold a significant data security advantage relative to detailed, signature-template-matching approaches. For the former, the design of the inspection system should not include any provision whatsoever for nonvolatile data storage. For the latter, several plausible approaches to preserving reference signatures have been identified, but agreement in the IBWG has not been reached about a preferred method. Since none of the current initiatives requiring IB technology foresee a demand for full-spectrum reference signature comparisons, consideration of the issues and plausible approaches for reference spectra protection is reviewed separately in an appendix to this report. The resolution of these issues will be undertaken at a later date.
- **Inputs and Outputs.** Consistent with the underlying need that all hardware and software must be inspectable, and all hardware and software functional modules and components must have a well-understood dedicated function, there must be no extraneous input or output ports or devices associated with the integrated radiation signature inspection system. In general, peripherals must be minimized and bus structures avoided (thereby requiring point-to-point direct connections).

- **Inspection System Authentication and Repair.** A very useful approach to assuring system functionality is the use of host-provided multiple copies, the minimum being two, from which the monitoring party selects one that it may take for thorough examination at home, and one for use under the inspection protocol. In the event of system malfunction due to faulty equipment, if the problem can be jointly localized by the host and the monitoring party, the defective module should be discarded and replaced. Replacement modules must be provided in duplicate for selection by the monitoring party (one to take home and examine, one to install). Detector head checks and repairs may be an exception to this guidance, however. Detector maintenance and repair may be afforded because such subsystems are easily inspected and do not normally contain digital electronics or significant amounts of analog circuitry.

The information provided in this report provides the basis for U.S. Interagency discussion of the technical topic, as well as providing important guidance to inspection system designers as they work to design and assemble prototype systems for demonstration deployment. This guidance is not intended to be a rigid recipe for the design and implementation of information barriers. Rather, it should be considered more as a standard against which proposed approaches to protect classified nuclear signatures or other measurement information under specific agreements are assessed.

Because the work of the IBWG is part of a larger effort that includes an independent assessment by a Security and Vulnerability Working Group (SVWG), independent validation of the design basis will come from the assessments conducted by the SVWG and other reviewers.

## CONTENTS

EXECUTIVE SUMMARY .....	3
CONTENTS .....	7
INTRODUCTION .....	9
I. INFORMATION BARRIER FUNCTIONAL REQUIREMENTS .....	11
II. INFORMATION BARRIER CRITICAL ELEMENT DESIGN BASES .....	13
A. Supplier of the Integrated System .....	13
B. Central Processing Unit (CPU) .....	14
C. Non-CPU Equipment .....	15
D. Procedural Issues .....	16
E. Tempest/Electronic Emanation Considerations .....	17
F. Optimal Location of Data Barrier(s) .....	18
G. Software, Firmware, CPU Operating Systems .....	18
H. Storage, Authentication, and Disposition of Non-Volatile Data Media .....	19
I. Inputs and Outputs .....	19
J. Authentication and Repair .....	19
REFERENCES .....	21
APPENDIX I. Bibliography and Summary of Recent Information Barrier Analyses .....	23
APPENDIX II. Excerpts from the FIPS PUB 104-1 Trusted Processor Software .....	25
Design and Documentation Guidelines	
APPENDIX III. Storage, Authentication, and Disposition of Non-Volatile Data Media ....	29
APPENDIX IV. Joint DOE-DOD Information Barrier Working Group Members and .....	31
Participants in February 1999 Design Basis Workshop	

(This page is intentionally blank.)

## INTRODUCTION

One of the most significant hurdles to overcome for further U.S.-Russian reciprocal reductions of nuclear weapons and weapons-useable fissile materials is that of cooperative monitoring in a manner that does not reveal classified weapons design information to a monitoring party. Over the last several months the U.S. Department of Energy has sponsored radiation signature measurement campaigns involving full-up nuclear warheads and warhead nuclear components. This effort was undertaken to gain advanced understanding of the effectiveness and limitations of using the nuclear radiation emanating from such objects as a means to help effect potential monitoring scenarios.[2] These campaigns are continuing. The U.S. Department of Energy has also begun to sponsor technical collaborations between U.S. and Russian nuclear weapons specialists looking at similar issues. It is clear that the use of radiation signatures can be a powerful tool in cooperatively monitoring warhead dismantlement, gaining confidence about the weapons origin of fissile material items in closed containers, tracking and safeguarding stored nuclear items and materials, and monitoring the disposition of nuclear materials from dismantled nuclear weapons. However, these same unique and useful radiation signatures by their very nature usually reveal too much information about the design the nuclear item being examined. The problem to be solved is that of somehow utilizing radiation signatures in a non-intrusive manner. Recent studies pertaining to this problem are listed in Appendix I.

To address this problem, the Departments of Defense and Energy jointly established the Information Barrier Working Group (IBWG) in late calendar year 1998 to devise optimal approaches to protecting classified nuclear weapons design information when utilizing radiation signature monitoring methods. [3] The membership of the IBWG is listed in Appendix IV. The current focus of these activities is on potential US-Russian (and IAEA) bilateral and trilateral agreements. It is important to note that at this writing the state of progress in the development of Trilateral Agreement monitoring equipment is well-advanced compared to the other two regimes, in anticipation of a mid-June 1999 demonstration to the IAEA and Russian Federation.[1] Information barriers may be needed for other agreements such as the Plutonium Production Reactor Agreement (PPRA), and the Plutonium Packaging and Identification Agreement (PPIA).

This report summarizes the results of a workshop held at Sandia National Laboratory in Albuquerque New Mexico during the period of February 2-4, 1999. The IBWG workshop was convened to establish the functional requirements associated with warhead radiation signature information barriers, to identify the major design elements of any such system or approach, and to identify a design basis for these major elements.

The information provided in this report provides the basis for Interagency discussion of the technical topic, as well as providing important guidance to inspection system designers as they work to design and assemble prototype systems for demonstration deployment. This guidance is not intended to be a rigid recipe for the design and implementation of information barriers. Rather, it should be considered more as a standard against which proposed

approaches to protect classified nuclear signatures or other measurement information under specific agreements are assessed.

## I. INFORMATION BARRIER FUNCTIONAL REQUIREMENTS

The basic, top-level functional requirements for the information barrier portion of an integrated radiation signature-information barrier inspection system are twofold:

1. The host must be assured that his classified warhead design information is protected from disclosure to the monitoring party, and
2. The monitoring party must be confident that the integrated inspection system measures, processes, and presents the radiation signature based measurement conclusion in an accurate and reproducible manner.

In the absence of any agreement to share classified nuclear weapons design information in the conduct of a monitoring regime, the requirement to protect host country classified warhead design information is fundamental and admits no tradeoff versus the confidence provided to the monitoring party in the accuracy and reproducibility of the measurements. This principle shaped the deliberations of the IBWG.

The fundamental requirement to protect classified information can be expanded into more descriptive, though top-level, requirements. Hamilton and Wood have suggested that the information barrier must

- protect the system from unauthorized operations and use
- prevent the unauthorized disclosure of classified data
- prevent the unauthorized and undetected modification of the system hardware and software, including the unauthorized modification, substitution, insertion, or deletion of classified data,
- employ approved yet transparent (i.e., unclassified) security methods for the protection of the classified data
- provide indications of the operational state of the system without revealing classified data
- detect errors in the operation of the system and prevent the compromise of classified data as a result of these errors. [4]

The standards to which the information barrier portion of an inspection system must be designed are described in the next section on critical element design. It is not possible at this time to discuss the functional requirements for any specific integrated inspection system, because 1) it is still the subject of ongoing and future negotiations, and 2) it depends heavily on the ability of radiation detection system developers to demonstrate capabilities. Such specific requirements will be the subject of reports by others charged to develop and demonstrate the various radiation signature systems.

(This page is intentionally blank.)

## **II. INFORMATION BARRIER CRITICAL ELEMENT DESIGN BASES**

The IBWG reached agreement on the enumeration of ten critical design elements that define a general standard for radiation signature information barrier design. Reasonable agreement was also reached on a recommended design basis (or "concept") for the critical elements needed for information barriers for the Trilateral Agreement, the Mayak FMSF Agreement, and the next round of START type negotiations.. These design elements are described below in loose order of relative importance to the working group. This order is not particularly significant, but the process was useful in addressing the issues, and the order suggests something about the logic behind the conclusions.

Because the work of the IBWG is part of a larger effort that includes an independent assessment by a Security and Vulnerability Working Group (SVWG), the following design basis descriptions are not detailed in their justification. Nor is significant space given to describing the shortcomings of alternatives in order to validate our conclusions and recommendations. Validation or criticism will come from the assessments conducted by the SVWG and other independent reviewers.

In this report, the term “integrated system” is used to denote the combination of the radiation signature inspection system design with the design principles, procedures, and special equipment required for an information barrier. The focus of this report is the use of such equipment under cooperative bilateral or multilateral agreements having to do with full-up nuclear warheads, containerized nuclear components removed from warheads, and altered shapes of or canned weapons-useable fissile material derived from such components. The shorthand term “warhead items” is used to denote the complete range of these inspectable objects.

### **A. Supplier of Integrated Measurement System and Information Barrier**

With the primary functional requirement for the use of an integrated radiation signature measurement and information barrier system being the absolute protection of host country classified weapons design information, determination of who supplies the equipment becomes a primary design issue.

There are basically three alternatives: monitoring party supplies the equipment, host country supplies the equipment, or a mixed approach. The term "supply" needs to be precisely defined. "Supply" in this case is defined as last extended, private access to the equipment just prior to its use on classified objects or materials. Private access to the equipment, of course, gives a party the opportunity to illicitly alter the equipment in some advantageous manner. For all three of these alternatives, it would be important to the degree politically acceptable for technical specialists of all parties involved to work together to provide the integrated system(s). With this, the technical concerns and preferences of each side could be addressed and solved early, providing the greatest degree of trust and transparency possible in the deployment of such potentially intrusive equipment.

The IBWG concludes that the best approach to protecting classified data from radiation measurement equipment is that of the host country supplying the equipment. Advocates of this approach argue that in using computer-controlled hardware such as radiation spectrometers, the risk of a supplier illicitly embedding undetectable, subtle indicators of classified information is too great. Host supply of the monitoring equipment is arguably the least problematic to carry to the negotiating table, and the least problematic in winning the approval of security and vulnerability assessment teams for actually using the equipment.

Operational safety is also an overriding concern to consider when addressing this issue. Again, it is deemed highly problematic to mollify weapons safety considerations for monitor-supplied equipment. Safety certification of equipment, particularly electronic equipment involving high voltages, is typically a protracted, detailed process when full-up nuclear warheads are to be examined.

It is important to qualify this approach. Host-country supply of the equipment as defined in this assessment does not negate, at all, the possibility that the monitoring party takes a primary role in designing, developing, and procuring any integrated measurement system. It is the issue of extended private access to the equipment just prior to its use that is pivotal. It is presumed that once the equipment is jointly put into use, it will be stored under some form of joint-custody arrangement.

It is conceivable that some radiation inspection equipment may need to be utilized under what is referred to as the "mixed" approach. Under some inspection situations, the monitoring party could show up with its own radiation measurement devices, and these could be examined in their presence by the host country. One variation of this approach is a process whereby two identical systems are offered to the host. The host could choose one at random for its own protracted security assessment, and allow the other to be used. Procedures can also be envisioned where the electronic radiation measurement equipment is discarded by the inspectorate after use (left behind with the host), such as for very inexpensive devices, or when reasonably sophisticated systems are used to initialize particularly sensitive nuclear warhead items. There are precedents for these approaches under the Intermediate Nuclear Forces (INF) Treaty, as well as the Threshold Test Ban Treaty (TTBT) Joint Verification Experiment (JVE).

With the determination that host-country-supplied monitoring equipment is the best design approach to assure protection of classified information, the primary consideration associated with the remaining critical design elements is enabling the monitoring party to be confident that the equipment performs as originally designed for the purposes intended.

## **B. Central Processing Unit (CPU)**

The recommended approach to selecting an overall system CPU or a set of processors sequenced in the classified data stream is that of dedicated, trusted processor architecture.

The concept of a trusted processor is a hardware and software architecture that is dedicated to the specific processing task(s), having extraneous functionality minimized or eliminated which makes it more readily inspectable. Commercially available single-board computers are good platforms from which to design the trusted processor for warhead components and materials monitoring applications.

Many of the U.S. prototypic radiation signature systems being studied at this time for potential application to nuclear warhead dismantlement, reduction, and disposition agreements employ laptop or desktop computers. The United States has used these systems in demonstrations on containerized, classified warhead nuclear components for Russian visitors. The advantages of using laptop- or desktop-based data processing subsystems are that they are relatively inexpensive, and they may be programmed to perform sophisticated processing using ubiquitous and multi-functional, commercially available operating systems.

It is the conclusion of the IBWG that laptop and desktop CPU systems would probably be too difficult to inspect to gain adequate confidence that additional, illicit functionality had not been incorporated by the host country. (The same perspective and concern would be likely be held by a host country for equipment supplied by an inspectorate). It would be exceedingly difficult, if not impossible, for the monitoring party to be assured that a deployed system using this equipment is truly performing as expected. And even though the host country would be "supplying" the integrated measurement system(s), in fact, it might very well be that the United States or IAEA would wish to provide such system to a Russian partner. It would be conducive to the success of such arrangements, if the Russian host would not find it overly difficult to privately examine such equipment.

Trusted processors are more easily inspected. For this and other reasons, they are often used for a variety of commercial data security applications. There are commercially available products that meet National Institute of Standards and Technology (NIST) standards for the protection of sensitive data of this type.[5] The applicability of commercially available trusted processors assembled for commercial security would need to be assessed for use as part of an integrated radiation signature information barrier CPU applied to warhead items. In any event, the design principles on which such systems are based are very relevant to this problem.

### **C. Non-CPU Equipment**

The design considerations associated with the CPU are also relevant to non-CPU elements such as the detector subsystem, and the detector signal pulse-height or multi-channel analyzer (MCA) subsystem.

The IBWG is in general agreement that the use of commercially fabricated and procured detector subsystems, such as a high-purity germanium (HPGe) detector with an integrated analog pulse preamplifier and liquid nitrogen dewar, are inspectable. It is advised that the preamplifier not be placed inside the dewar, as some are for low noise applications, in order to facilitate security and functionality examinations. It is believed that rigorous examinations of

integrated detector subsystems can be achieved using portable x-ray equipment. In many instances confidence could also be offered procedurally by the offering and random selection from two or more detector subsystems. For reasons that are discussed in Section II.E., it is also recommended that the detector subsystem be well-shielded from radio-frequency interference.

The inspectability of additional analog electronics and multi-channel analyzers needs to be evaluated on a case-by-case basis. But because these systems are not as sophisticated as the CPU, it is believed that the integrated system design teams should be able to work with commercial suppliers to provide inspectable, dedicated MCA devices. The same conclusion applies to power supplies, and to analog pulse shaping amplifiers -- all standard subsystems in spectrometric radiation measurement systems.

In general, the inspectability of radiation measurement systems being considered for nuclear arms reduction applications decreases as the sophistication and complexity of the system increases. Design teams and others advocating the use of complex systems must configure nearly every electronic element of their system to maximize overall system inspectability.

#### **D. Procedural Issues**

The procedural problem that must be addressed is how to keep a monitoring party from deducing sensitive information about the fissile material being examined simply as a result of the conduct of the inspection itself, rather than from the data collected. This need must again be assessed on a case-by-case basis. A particular problem is that detector placement and utilization. The guidance in this case is that the instrument should be able to autonomously determine and use the optimum counting time, geometry, etc., with the details of this process concealed by the IB.

For most types of radiation-signature-based inspection systems, the detector subsystem must be placed next to the item being inspected in a manner assuring that the count rate is neither too high nor too low for proper function of the system. Because the design details of the inspection system will be well-understood by all parties, certain sensitive information might be deduced about a warhead or component by the mere setup of the equipment if care is not taken. The problem that must be addressed is how to keep a monitoring party from deducing sensitive information about the quantity of fissile material being examined, knowing what the detector efficiency is, being able to observe the distance from the object, as well as being able to observe the length of time it takes the measurement system to reach a conclusion.

Certainly there may be some inspection regimes, such as in the case of Mayak FMSF, where the quantity of material being examined is not sensitive. But in any regime where the material quantity is classified, a component of an effective integrated information barrier is a detector system that is autonomously autoscalable. In order to accomplish this, the integrated system must perform measurements for a fixed counting time. If adjustments are required,

they should be performed autonomously and in a way that cannot be determined by an observer.

## **E. TEMPEST/Electronic Emanation Considerations**

It is important under the condition of host-supplied inspection equipment that the host is assured that there are no electronic or optical emanations from the measurement system that the monitoring party can record. Likewise, the monitoring party must have a high degree of confidence that the host can not somehow control or adversely affect the proper operation of the inspection system during an actual measurement or calibration.

In order to help assure the complete protection to classified design information, it is recommended (and assumed for the purposes of this report) that the classified objects being inspected are within the boundary of the host country, and are within host-controlled facilities. Under such conditions, it is also assumed that people entering the staging or storage areas where measurements are to be made will be checked to assure they are not carrying any unsafe objects or any electronic equipment not permitted by the relevant inspection protocol. Such procedures when combined with standard good design practice in minimizing electronic emanations are believed sufficient to effect the necessary high degree of information security required of the integrated system. TEMPEST standards need not be applied for the protection of the information under these conditions.

The more troublesome problem under these conditions is assuring that the host country is not affecting the operation of the system illicitly using some form of radio control. The use of dedicated trusted processor designs with well-understood control software, combined with a general approach of complete transparency in any integrated inspection system design, are necessary to help assure the monitoring party that the host can not illicitly control or affect inspection measurements.

It is interesting and problematic that often the simpler measurements, such as integrated (total) count rates are probably more susceptible to radio-induced control than more complex measurements such as high resolution gamma spectrometry. It is believed that integrated neutron emission rate measurements, a preferred approach for determining item mass, using He-3 gas ionization type detectors are particularly susceptible to illicit radio control. It is a well-known problem among experimentalists that a burst of electronic interference from an object such as a handheld radio can result in a burst of "counts" from such a detector. This situation could easily lead the monitoring party to believe that there are many more neutron emissions than there actually are, and thus much more material present than there actually is. Such radio bursts are less likely to adversely affect solid state detectors, such as used for gamma-ray spectrometry. What effects that might occur would likely significantly alter the overall measured spectrum shape, perhaps even to the point that spectral algorithms would not function properly.

With an understanding that all the electronic elements and subsystems of a radiation measurement and data analysis system will potentially show some degree of susceptibility to

radio interference and perhaps even radio control, the integrated system designer will have to take such possibilities into consideration. It is likely that the related security and vulnerability assessment associated with any system will, in the final analysis, primarily be an empirical process. Radiation measurement system designers of equipment slated for use in most any real-world environment, such as around a nuclear reactor or near a particle accelerator, are well versed in how to minimize radio-interferences. The degree to which good radio-frequency-interference (RFI) design practices will need to be implemented, even to the degree that the whole measurement system must be fabricated to stringent TEMPEST standards, will depend on the results of empirical vulnerability assessments and also to the subjective degree a monitoring party wishes to minimize this risk. However, the protection of the classified design information will not be heavily dependent on radio emission considerations under the host-controlled scenario.

#### **F. Optimal Location of Barriers(s)**

In the circumstance where there is little measured data that is not classified, such as that associated with radiation emanations from warhead items, some additional security may be afforded through the use of intermediate barriers. While a layered data security approach is appealing, it is difficult to conceive of filters which could be effective in completely alleviating data security concerns for these types of inspection systems used for these purposes. At the same time, employing intermediate filters can be detrimental to checking system functionality. If intermediate barriers can be employed without compromising functionality assurances, then it may be desirable to do so. Ultimately, it is at the system level that information security (including system use procedures) must be assessed, however.

It is certainly a valid design principle to filter unneeded data as early in the acquisition and analysis sequence as possible. However, while certain data may not directly contribute to an attribute analysis (such as Pu240/Pu239), portions of the spectrum lying outside that necessary for determining the attribute might be very important to automatically check system function, or validate the measurement process.

#### **G. Software, Firmware, CPU Operating Systems**

In the situation where the host country supplies the integrated radiation signature inspection system, there is still the risk of compromising classified information through either planted or inadvertent computer code quirks of system operation. Similarly, there is considerable risk to the monitoring party that the system can be surreptitiously controlled or otherwise caused to give misleading or incorrect results if the system computer code cannot be examined adequately because it is proprietary or too complicated. Just as the data processing hardware must be completely inspectable, so too must the associated computer codes. The complete inspectability of the data processing hardware and software is critical to the trusted processor design concept.

To negate the risk of compromising classified information, and to minimize the risk of host-country surreptitious interference with the operation of the radiation signature inspection system, the code in the form of firmware, applications software, or software operating system must be inspectable. This necessitates that the amount of code be limited and that there be no extraneous code. It also suggests that complex high-level software operating systems not be utilized. This does not necessarily negate the use of compiled analysis code. In Appendix II of this document, excerpts are reproduced from the Federal Information Processing Standards Publication (FIPS-PUB) 140-1, Security Requirements for Cryptographic Modules. The software design principles documentation requirements excerpted, as well as other information provided in the referenced publication, are directly applicable to the protection of warhead-related data.

## **H. Storage, Authentication, and Disposition of Data and Data Media**

Unclassified attribute-based inspection systems hold a significant data security advantage relative to detailed, signature-template-matching approaches. For the former, the design of the inspection system should not include any provision whatsoever for nonvolatile data storage. For the latter, several plausible approaches to preserving reference signatures have been identified, but agreement in the IBWG was not reached about a preferred method. Since none of the current initiatives requiring IB technology foresee a demand for full-spectrum reference signature comparisons, consideration of the issues and plausible approaches for reference spectra protection is reviewed separately in Appendix III. The resolution of these issues will be undertaken at a later date.

## **I. Inputs and Outputs**

Consistent with the underlying need that all hardware and software must be inspectable, and all hardware and software functional modules and components must have a well-understood dedicated function, there must be no extraneous input or output ports or devices associated with the integrated radiation signature inspection system. It is difficult to state on a general basis specifically what I/O is required, because that will depend on the actual radiation detect system. But for Yes/No type results output, it is recommended that only simple displays be used, e.g.: a 2-line LCD display, as opposed to video displays. And in general, peripherals must be minimized and bus structures avoided (thereby requiring point-to-point direct connections). The advantage of using dedicated I/O ports is that their use can be more easily located in software, making the system more inspectable.

## **J. Inspection System Authentication and Repair**

A very useful approach to assuring system functionality is the use of host-provided multiple copies, the minimum being two, from which the monitoring party selects one that it may take for thorough examination at home, and one for use under the inspection protocol. The latter would forever be located at the host's location under dually applied physical

security arrangements. Prior to the first time a particular type of inspection system is utilized, a copy of all software must be provided to the monitoring party by the host so the monitoring side can thoroughly review it and devise ways to authenticate this software installed on the actual inspection system. It is more problematic to determine the same degree of similarity between hardware subsystems, but it goes without saying that the inspecting side and the hosts will agree to completely share the design features, for example, through exchange of detailed technical drawings.

In the event of system malfunction due to faulty equipment, if the problem can be jointly localized by the host and the monitoring party, the defective module should be discarded and replaced. Replacement modules must be provided in duplicate for selection by the monitoring party (one to take home and examine, one to install). Detector head checks and repairs may be the exception to this guidance, however. Detector maintenance and repair may be afforded because such subsystems are easily inspected and do not normally contain digital electronics or significant amounts of analog circuitry. If the host and the inspector both suspect that a detector is malfunctioning, it can be removed and placed on a laboratory spectrometer system and the spectra from unclassified radioactive sources viewed in order to assure proper function. Joint control of any equipment module during evaluation and repair is mandatory.

In addition to these procedures, it would also be very useful if the monitoring party retained the right to periodically re-authenticate under joint custody the complete measurement system or any subsystem. The right of random re-authentication would be a very useful tool to a monitoring party in the situation where the equipment is retained under dual physical security in the host country.

## REFERENCES

1. *Functional Requirements for a Prototype Inspection System and Information Barrier for the Trilateral Initiative*, Duncan W. MacArthur and Rena Whiteson, LA-UR-99-829, February, 1999.
2. *(A U.S. classified report)*.
3. Letter to Distribution from Rose Gottemoeller, Joint DOE/DOD Integrated Technology Plan, February 3, 1999.
4. *An Information Security Approach to Information Barriers for Radiation-Based Verification of Classified Materials*, Victoria Hamilton and Bradley Wood, Sandia National Laboratories, Albuquerque, NM, January 27, 1999, to be published.
5. *Security Requirements for Cryptographic Modules, Federal Information Processing*, Standards Publication FIPS PUB 140-1, U.S. Department of Commerce, National Institute of Standards and Technology, January 11, 1994.

(This page is intentionally blank.)

## **APPENDIX I. Bibliography and Summary of Recent Information Barrier Analyses**

*CIVET – a Controlled Intrusiveness Verification Technology*, Caesar Sastre, J. Sanborn, and J.P. Indusi, Verification Technologies, U.S. Department of Energy, March/April 1991.

*Transparency and Verification Options: An Initial Analysis of Approaches for Monitoring Warhead Dismantlement*, USDOE Office of Arms Control and Nonproliferation, May 19, 1997, Official Use Only

*Information Barriers*, B. D. Geelhood and J. L. Fuller, PNNL-12097, March, 1998.

*Information Barriers in the Trilateral Initiative*, D.W. MacArthur and R Whiteson, LA-UR-98-2137, May, 1998.

*Information Barriers to Protect Sensitive Nuclear Weapons and Materials Inspections*, B. D. Geelhood, PNNL-11982, September 2, 1998.

*Functional Requirements for a Prototype Inspection System and information Barrier*, R. Whiteson and D. W. MacArthur, LAUR-98-5982, 1998.

*Functional Specifications for a Prototype Inspection System and Information Barrier*, Duncan W. MacArthur, Rena Whiteson, and Robert P. Landry, LA-UR-99-1174, March, 1999.

*An Information Security Approach to Information Barriers for Radiation-Based Verification of Classified Materials*, V. Hamilton and B. Wood, SNL Submission to INMM, 1999.

(This page is intentionally blank.)

## **APPENDIX II. Excerpts from the FIPS PUB 140-1 Trusted Processor Software Design and Documentation Guidelines**

The following guidelines are useful in clarifying selected aspects of developing a trusted processor. The reader is referred to the comprehensive standard for complete specifications, especially as related to any cryptographic elements that might be required. [5]

### 1. Recommended Software Development Practices.

The following programming techniques should be used to facilitate analysis of the program, and to reduce the chances of programming errors. Deviations from these practices may be appropriate in some instances.

- Each variable should have an associated comment that gives the range of allowable values for the variable. If the range is unrestricted, this should be noted.
- Each procedure should have only one entry point. Each procedure should have at most two exit points, one for error exits and one for normal exits.
- Control flow within a procedure should be defined using only the following constructs: sequence, if-then-else, while-do, case repeat-until, for, and other structured loop constructs.
- Data should be communicated between procedures through the use of argument lists and/or explicit return values. Global variables should not be used except where necessary for the implementation of an abstract data type.
- Modules (which consist of data plus one or more associated procedures) should be constructed according to the principle of encapsulation/information-hiding.
- Each loop should be preceded by a convincing argument (as a comment) that termination is guaranteed.
- Each procedure should perform only a single, well-defined function.
- Each procedure should be preceded by a comment explaining the function performed by the procedure.
- Floating point comparisons should not be used.
- Where possible, variable names should be used to permit multiple memory usage for conflicting purposes.
- Upon entry to a procedure, input parameters should be checked for appropriate values where possible.

- The software should be hierarchically structured as a series of layers.

The following additional programming practices should be used when the implementation is in assembly language. Deviations from these practices may be appropriate in some instances.

- All code should be position independent, except where appropriate security concerns, efficiency or hardware constraints require position dependency.
- All register references should use symbolic register names.
- Self-modifying code should not be used.
- All procedures should be responsible for saving and restoring the contents of any register, which is used within the procedure.
- Control transfer instructions should not use numeric literals.
- Each unit should contain comments describing register us in the unit.

## 2. Recommended Software Documentation Practices.

Designers should be prepared to supply the following documentation to assure the inspectability of trusted processors used in the radiation signature measurement system.

### Module Interfaces.

- Specification of the interfaces of a cryptographic module, including any physical or logical ports, physical covers or doors, manual or logical controls, physical or logical status indicators, and their physical, logical, or electrical characteristics.
- Specification of the set of authorized maintenance procedures for the module.
- Specification of the defined input and output data paths.

### Roles and Services.

- Specification of all of the authorized roles supported by the module.
- Specification of each of the authorized services, operations, and functions that can be performed with the module. For each service, the service inputs, corresponding service

outputs, and the authorized role (or set of roles) in which the service can be performed, shall be specified.

#### Finite State Machine Model.

- Specification and description of all states of the module and of all the corresponding state transitions. The descriptions of the state transitions shall include the internal module conditions, data inputs and control inputs that cause transitions from one state to another, and shall include the internal module conditions, data outputs and status outputs resulting from transitions from one state to another.
- Finite state diagrams in sufficient detail to assure the verification of conformance to this standard.

#### Physical Security.

- Specification of the physical embodiment and security level for which the physical security mechanisms of a cryptographic module are designed, and a description of the applicable physical security mechanisms that are employed by the module.
- Specification and description of the environmental failure protection features employed within a module, or of the environmental failure tests performed and the results of those tests.

#### Software Security

- Specification of any software or firmware that is excluded from the software security requirements, and explanation of the rationale for the exclusion.
- Detailed description of the design of the software within the module (e.g., the finite state machine model specification).
- Complete source code listing for all software contained within the module. For each software module, software function and software procedures, the source code listing shall be annotated with comments that clearly depict the relationship of these software entities to the design of the software.
- Annotations in the source code listing for each software module, software function and software procedure, clearly specifying (1) the pre-conditions required upon entry into the module, function or procedure in order for it to execute correctly, and (2) the post-conditions expected to be true when execution of the module, function or procedure is complete. These conditions may be specified using any notation that is sufficiently

detailed to completely and unambiguously explain the behavior of a module, function or procedure.

- Detailed explanation (informal proof) of the correspondence between the software design (as reflected by the pre- and post-condition annotations) and the formal model

#### Self-Tests

- Specification of each possible error condition, including the conditions and actions necessary to clear the error and resume normal operation (possibly to include maintenance, servicing or repair of the module).
- Specification of all critical functions, and the nature of the power-up self-tests designed to test those functions.

### **APPENDIX III. Storage, Authentication, and Disposition of Non-Volatile Data Media**

The storage and disposition of nuclear warhead data is a very important factor to consider in the construct of inspection protocols and the design of the integrated inspection systems. It is clear that unclassified attribute-based inspection systems hold a significant data security advantage relative to detailed signature template matching based approaches. For the former, the design of the inspection system should not include any provision whatsoever for nonvolatile data storage. Such writable media are unnecessary and could create significant unwarranted additional data security risk. In effect, the unclassified attributes constitute an unclassified set of parameters (a rudimentary template) against which analyzed data from an inspected item is compared and a conclusion reached.

However, in some situations, classified templates offer advantages. For example, they offer the possibility of dismantlement verification at the warhead type/class level [2]. They also may be used to leverage to great advantage a detailed procedure-based initialization process to identify items. Detailed energy and time-domain spectral comparisons offer the promise of high confidence item identification and tracking. The major disadvantage of such approaches and systems is that the use of a classified reference spectrum is required. Such an approach requires the recording, storage, and disposition of potentially highly data. The manner in which such a process can be effected is problematic.

The trusted storage and disposition of reference template spectra is an issue on which the IBWG did not reach agreement at the time this design basis report was issued. It will require an assessment by national security authorities who will likely not be in a position to completely reveal their reasoning, but who will be recognized at least within the United States as having the authority and expertise to do so.

There are at least four basic methods to store reference inspection data in a secure manner. Two of these methods afford maximum protection of host-country information, but also maximize risk to the monitoring party of reference data tampering by the host. The other two methods provide a very high degree of protection against host country tampering, but intuition suggests that negotiability may be a significant problem. All four methods have as a central element the use of a trusted processor to encrypt the full template or addend an encrypted, unique data tag to any reference template to be stored for later use. [4]

Four plausible approaches to protecting reference warhead related radiation signature templates presented at the workshop are:

1. Fully encrypted reference data set given to monitoring party for safe keeping at use at subsequent inspections, host keeps possession of trusted encryption processor and encryption key
2. Tagged/signed data set retained by host along with private key, zeroed trusted processor retained by monitoring party

3. Host retains both signed/tagged data set and trusted processor; monitoring party utilizes time-sensitive private key to validate reference data
4. Host retains both trusted processor and signed/tagged reference data under dually applied physical security; monitoring party retains private key to validate reference data.

Approach 1 may appear to be highly imprudent. But in fact, encrypted nuclear weapons data and other U.S. national security information is transmitted by interceptable telecommunications every day. The similarity of this to that of physically handing a monitoring party a encrypted data disk containing a classified radiation signature template or templates must be reviewed by the proper U.S. Government authorities and a policy decision reached in order to provide guidance to both U.S. delegations and integrated signature system designers.

Indeed the vulnerability and concomitant risk associated with either Approach 1 or 2 must be reviewed by the proper U.S. Government authorities, and guidance provided. It is more intuitive to argue that maximum data protection is afforded by retention of the both the template data and the trusted processor by the host. (The processor in this case is a unit used for tagging the data through privately keyed hash function procedures, and then again using a public key to validate the reference template(s)). The concern regarding these two approaches is that of monitoring party confidence that the reference data left behind in the host country is not illicitly altered before it is used again in a future inspection. Given the inviolate functional requirements on the integrated radiation signature measurement system (absolute confidence that no classified data is at risk relative to reasonable confidence that the inspection system is functioning properly), and given the fact that many encryption methodologies have been shown to be vulnerable with enough time and effort, the ultimate U.S. Government and Russian choice in the matter of reference data storage is likely to be quite subjective.

A less esoteric problem concerns the disposition of template data or the data comprising the private key (which is used to generate the template tag). A fundamental design constraint is that the trusted processors contain no non-removable, non-volatile data storage media. Even so, guidance is required from U.S. Government authorities on the most acceptable method to zero volatile media that has contained either the private hash function data tagging key or the classified radiation signatures.

**APPENDIX IV. Joint DOE-DOD Information Barrier Working Group Members and Participants in February 1999 Design Basis Workshop**

**Members**

Thomas Bowman	DTRA/OSPCT
Andrew Carlson	NSA
Richard Comerford	DOE.NN-522
Thomas Duham	DTRA
Leon Foreman	BNL
James Fuller, Chair	PNNL
Bruce Geelhood	PNNL
William Johnson, Deputy Chair	LANL
Wayne Kiehl	Pantex Plant
Marshall Kohen	DOE/NN-513
David Lee	DTRA/OSPCT
Duncan MacArthur	LANL
Dean Mitchell	SNL
James Mullens	OR/Y12 Plant
James Wolford	LLNL

**Additional Participants, February 2-4 Meeting at SNL**

Tom Barger	SNL
James Boyle	DTRA
Peter Chiaro	ORNL
Thomas Gosnell	LLNL
Victoria Hamilton	SNL
Charlie Harmon	SNL
Hunter Lutinski	DTRA
Paul Mann	SNL
Keith Marlow	SNL
Harless McDaniel	DTRA
Horace Poteet	SNL
Gerry Quinlan	SNL
Hugh Scott	SNL
Douglas Smathers	SNL
Andra Stoller	DTRA
Keith Tolk	SNL
George West	Pantex Plant
Gregory White	LLNL
Bradley Wood	SNL
Peter Zuhoski	BNL