Information Barriers for the Protection of Sensitive Information

Arden D. Dougan, Michele Smith,
David Beach, Justin Clinton, John Dunn, Kevin Seager,
and Peter Vanier

U.S. Department of Energy
National Nuclear Security Administration (NNSA)

Seventh Joint ESARDA/INMM Workshop on Future Directions for Nuclear Safeguards and Verification

October 17, 2011 Aix-en-Provence, France
What is an Information Barrier?

- An Information Barrier is a combination of technology and procedures that prevent the release of host-country sensitive information to a monitoring party during an inspection of a sensitive item, while enabling assurance of an accurate assessment of host country declarations regarding the item.

  - Based on U.S. Information Barrier Working Group definition, circa 2000

  - Historical basis dates to 1990s, including R&D associated with the U.S.-Russia Mutual Reciprocal Inspection agreement, the Trilateral Initiative and Mayak Fissile Material Storage Facility, and the commitment by Presidents Clinton and Yeltsin during the 1997 Helsinki Summit to pursue transparent and irreversible strategic arms reductions
Competing goals within the framework of a monitoring regime

Monitored Party/Host

Protection of sensitive information

Certification

The process through which the host is convinced that its sensitive information is adequately protected.

Monitoring Party

Confidence in measurement

Authentication

The process by which a monitoring party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item.

Authentication builds confidence
Can technical approaches ease the conflict of goals in a monitoring regime?

- Clearly competing goals in a monitoring regime may never be fully reconciled.

- Confidence can be increased for both parties by implementing technical and procedural measures.

- The monitored party’s concerns may be addressed by certification and implementation of information barriers.

- The monitoring party’s concerns may be addressed by implementing authentication procedures throughout the technology development.

- Joint development and demonstration of equipment and procedures can help address both parties’ concerns.
Information Barrier: a combination of technology and procedures

- Permits necessary measurements and provides useful results without revealing sensitive information
- Allows monitors to authenticate that the instrument is performing correctly

**Notional block diagram of an information barrier**

Sensitive measurement results are compared to a non-sensitive threshold value to obtain a non-sensitive pass or fail result.
Certification and Authentication

- **Certification**-
  The process through which the host is convinced that his sensitive information is adequately protected.

- **Authentication**-
  The process by which a monitoring party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item.

These two tasks require different tools and are performed by different people, but share some concerns in common.
Certification and authentication are complementary concepts

Host and monitor share an interest in reliable hardware, software and human procedures.
Information Barrier Design Guidelines

• Each element – simple, transparent and justifiable
• Modular construction
• Defense in depth – independent layers of protection
• All hardware elements and software source code should be available for inspection
• Well documented system design
First Generation Information Barriers

- **Joint Verification Experiment/CORRTEX system, 1988**
  - US/Russian collaboration on Threshold Test Ban Treaty monitoring
  - Demonstration of yield threshold monitoring during actual U.S. and Soviet nuclear tests (sensitive data protected)

- **BNL Controlled Intrusiveness Verification Technology, CIVET, 1992**
  - Demonstrated use of a simple custom-built computer to control precise HPGe measurements for template matching
  - Concluded that Authentication and Certification required simplest hardware and software with no extraneous capability

- **Mutual Reciprocal Inspection Talks, 1994**
  - Spectral segmentation (e.g., Pu-600 approach) developed

- **Trilateral Initiative integrated system demonstration at LANL, 1999**
Second Generation Information Barriers

- SNL Trusted Radiation Attribute Demonstration System (TRADS), 2000
  - Demonstration of novel trusted processor

- LANL/LLNL Fissile Material Technology Demonstration (FMTTD), 2000
  - Fully certified demonstration system
  - Used on actual U.S. weapon component for Russian audience
Recent Information Barriers

- **UK-Norway, 2010**
  - Non-nuclear weapon state (played by UK) verifying warhead dismantlement of nuclear weapon state (played by Norway);
  - Mock weapon used $^{60}\text{Co}$ as fissile component
  - Both parties constructed prototypes based on joint design
  - Modular construction, commercial-off-the-shelf electronic components

- **U.S.-Russia Attribute Measurement System, 2010**
  - Verification of containers of plutonium (3 attributes)
  - Commercial-off-the-shelf where possible
  - Secure mode and open mode
Comprehensive Nuclear-Test-Ban Treaty – On Site Inspection Spectral Blinding

- Relevant radionuclides must be **reliably identified, and quantified** to assess whether a nuclear explosion has occurred

- Information Barrier could be used to show only relevant radionuclide data from radiation measurements
  - Raw spectral data not shared

- Gamma-spectroscopy of mixed fission products can be very complex

*There are significant information barrier challenges; analysis must quantify amounts present in highly variable field and background conditions*
International Safeguards - Mailbox

- To provide after the event notification of material movement within a facility

- **Protection of proprietary data**
  - Data filtered prior to sending
  - Secure, electronic transfer from facility to IAEA
  - Yes/No or Anomalies

- **Inspectors access Mailbox during Unannounced or Short Notice Random Inspections**

- **Mailbox could be a key piece of remote inspections**
  - Provide declaration to IAEA
  - Check against remote data
Emerging challenge – imaging data

Detect diversion of fissile material from sealed storage containers
Not all information about images and energy spectra may be disclosed

- Object of interest
- Storage container
- Sealed container
- Inspection
- Analysis algorithm
- Yes/no result
- Information barrier
- One number
- Unclassified metrics for comparison
- Sensitive images of internal structure with full energy spectra per pixel

Available data:

Imaging is under consideration as a powerful, but potentially invasive tool
Material recognition incorporates spectral and spatial information

- Item discrimination based upon density and atomic number
- Verifies presence or absence of material (not necessarily quantity)
- PNNL is improving material recognition capabilities to include knowledge of geometry, numerical approaches like principal component analysis (PCA), and assumptions based on edge transitions

Pu Storage Container (transmission image)  Estimated Material Densities
Algorithm Development: Histograms

- Compare pixel-intensity histogram of observed image to reference
- Histogram intended to be a non-sensitive reduction of image, which can be stored outside an IB
- PNNL is determining whether sensitive parameters can be determined from the histogram
  - If no, storing reference histogram as template may be acceptable
  - If yes, no storage allowed
Perceptual Hashing: Image Fingerprint?

- PNNL is examining “one-way transforms” for comparison of robust to minor image variations (noise, rotation, compression, geometric distortion, filtering)

- Example:

- Perceptual “hashing” is NOT traditional (cryptographic) hashing—same or very similar output for similar images
Conclusions

• **Information Barrier concept has matured**
  – Initial concepts for arms control explored and developed in 1990s
  – Greater balancing of certification and authentication in design evolution
  – Concept in use in other fields beyond arms control and safeguards

• **More complex data and technologies will be more difficult to implement, certify and authenticate**

• **R&D is needed for improved algorithms and authentication techniques**
  – Fully certifiable and authenticable system remains to be developed
  – Other verification tools with IBs to be explored further

• **Joint development and demonstration can enhance confidence and help balance certification and authentication requirements**