BNL-100981-2013-IR

Information Filters for Safeguards Applications: A Scoping Study

Katherine Bachner & Dawn Verdugo

May 2013

Nonproliferation & National Security Department
Brookhaven National Laboratory

U.S. Department of Energy

Notice: This manuscript has been authored by employees of Brookhaven Science Associates, LLC under Contract No. DE-AC02-98CH10886 with the U.S. Department of Energy. The publisher by accepting the manuscript for publication acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

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 any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use 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 its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Information Filters for Safeguards Applications: A Scoping Study

Katherine Bachner and Dawn Verdugo **PREPARED FOR THE U.S. DEPARTMENT OF ENERGY/NATIONAL NUCLEAR SECURITY ADMINISTRATION, NEXT GENERATION SAFEGUARDS INITIATIVE, CONCEPTS AND APPROACHES**

Prepared by Brookhaven National Laboratory

Information Filters for Safeguards

Scoping Study

Katherine Bachner & Dawn Verdugo, Brookhaven National Laboratory

May 2013

Table of Contents

1. Executive Summary: 4

2. Introduction to Information Filters 6

Terminology of Information Filters 9

a. How IFs have been used in the past 9

(1)Trilateral Initiative 9

(2) CIVET 11

(3) The AVNG System 12

(4) CWC Onsite Inspections 14

3. Current Generation Information Filters: The AVNG 2.0 15

AVNG: Current Status 15

B. The Norway-UK Initiative 16

5. Potential Application of the IF Concept in International Safeguards 17

General Challenges 17

A. Verification of Enrichment Plants 18

B. Complementary Access Inspections, Additional Protocol 19

C. IAEA's expanding role in arms control: the FMCT 22

6. Anticipated Implementation Concerns with IFs for Safeguards 22

Table 1: Comparative challenges that IFs could address 22

7. Safeguards challenges that could be addressed with IFs.....24
Existing safeguards challenges that could be addressed with IFs..... 24
Foreseeable safeguards challenges that might be addressed with IFs..... 24
8. Next steps and recommendations 25

1. Executive Summary:

A core concern of the Department of Energy is protecting sensitive information in the face of verification agreements that may make use of increasingly sophisticated and intrusive sensors. The conflict between intrusiveness and information protection is evident in existing treaties, such as the Chemical Weapons Convention (CWC) and the Additional Protocol (AP), where Congress has seen a need to step in and enact implementing legislation to protect, for example, sensitive information such as certain unique chemical signatures, but in so doing has introduced complexities into U.S. treaty compliance policy[1]. Information barriers or filters[2] (IFs) – broadly defined as physical and/or encryption mechanisms that preclude acquisition of sensitive, quantitative information while allowing the acquisition of treaty-relevant qualitative information by an inspectorate – could play a useful role in avoiding this type of conflict. In order to stimulate new thinking on ways to meet existing and future safeguard challenges, this scoping study investigates how IFs – a technique borrowed from the realm of arms control verification - might contribute to international safeguards activities.

Information filters[3] (IFs) have long been recognized as an important tool for the protection of sensitive signals and other data in the verification of bilateral and multilateral arms control treaties. The implementation of NPT safeguards, while differing somewhat in context from arms control verification, involves similar sensitivity concerns. This report examines whether or not IFs can be useful in the world of international safeguards, and provides a survey of methods of barring or filtering information that could be applied. The study finds that while many safeguards activities involve non-sensitive data, there are also a number of areas where IFs are already in use and others where IFs could make a useful contribution. Examples include verification of enrichment plants, complementary access inspections, and the Additional Protocol (AP) to

[1] Luke, John S. "Exploring the Possible Use of Information Barriers for Future Biological Weapons Verification Regimes", LLNL-SR-525091.
[2] Also referred to as information filters
[3] Often referred to as information barriers.

Comprehensive Safeguards Agreements (CSAs) under the Nuclear Non-proliferation Treaty (NPT).

This study considered a range of general safeguards activities, to see if there existed any unmet challenges that could be addressed by the inclusion of some method for information filtering. This study surveyed the following set of activities: verification of enrichment plants, Managed and Complementary Access inspections, and the IAEA's anticipated expanding role in arms control under the FMCT. The study found evidence that challenges within some of these current activities could be addressed by IFs, but the authors anticipate more specifically that future international safeguards activities might stand to benefit from a closer look at IFs. An in-depth study within a particular safeguards context is proposed, so the true costs and benefits to including an IF can be ascertained. The authors put forth the following preliminary recommendations to aid any future studies.

For one, while considerable effort has been directed toward addressing concerns about information barriers' authentication under the Trilateral Initiative, treating the issues of IF authentication in a safeguards context would be beneficial. One recommendation is to review the work that has been done in arms control on IFs and determine whether those existing authentication standards (1) are adequate; and (2) would be expected to satisfy potential IAEA safeguards needs.

Second, in the course of this scoping study, the authors found an unexpected aversion to certain terminologies associated with information filtering in a safeguards environment. 'Information barriers', the traditional term used in arms control applications, may need to be replaced with an innocuous term that would be acceptable to a larger international safeguards audience. The authors suggest addressing any such terminology issues with representatives from the IAEA and member states.

To address anticipated future safeguards challenges, the authors suggest connecting with one currently NGSI-funded initiative focused on expanding the Complementary Access Toolkit to include commercial-off-the-shelf chemical detectors. The detectors under consideration, often used in forensics and in-field environmental sampling, may present a much greater detection range than the gamma signatures obtainable by the current HM-5 detector. Some of these signatures might reveal commercial, proprietary processing information and could raise operators concerns. For a near-term demonstration of IF's suitability for a real-life safeguards scenario, the authors recommend working with those investigators to determine any points in a CA inspection that might benefit from inclusion of an IF. If an IF is deemed a practical addition, that team's upcoming field testing campaign could be augmented with a simplified IF. Such a demonstration seems like a cost-effective leveraging opportunity for two NGSI teams.

Finally, for in-depth consideration of an IF, the authors identify gas centrifuge enrichment plants (GCEP) as presenting an unmet safeguards challenge that information filtering could address. Gas centrifuge enrichment plants have overlapping verification points, where both safeguards data and proprietary facility operator data can be extracted. The specific safeguarding challenge is how to detect and verify undeclared feed in GCEP in the form of excess LEU production, while maintaining protection of operators' proprietary information. This study finds compelling evidence to suggest that GCEP is an area ripe for exploration of specific technical needs that could be met by IFs. This study

recommends undertaking further research directly relevant to the challenges and needs posed by GCEP relevant to international nuclear safeguards.

2. Introduction to Information Filters

IFs aim to provide confidence of treaty compliance, while protecting sensitive information. They comprise hardware, software, and administrative controls as a system to keep sensitive information from being revealed.[4] If the international safeguards community ascertained a need among inspectors to have access to information without access to sensitive data, IFs could present novel opportunities. IFs could provide a type of managed access to material requiring initial or confirmatory measurements located in a system that would normally require some level of protection (i.e., facility operator concerns over revealing proprietary information). While examining possible applications for IFs in safeguards, the main purpose of this scoping study is to determine whether such a need exists.

An IF is used in a measurement system that contains classified, proprietary, or other sensitive information to prevent the dissemination of the classified material while maintaining the ability for an inspector or verifier to come to their own conclusions about the contents, the procedures or the violations at issue.[5] The rationale for using an IF is that the person or institution verifying aspect *x* of a treaty or agreement must not have access to the item that they are verifying. The verifier seeks certainty that the claimed process or event has or has not taken place. At the same time, the party to be verified, for reasons of law, defense, commerce, or other sensitivities, cannot provide access to certain information integral to the verifier's search. This tense dynamic requires technologies that can balance the requirement for information with the requirement not to disseminate sensitive information. Either a simple IF that provides a yes/no answer, or a complex one that seeks to provide a more detailed method of obscuring certain data can meet that need.

Exploring the suitability of IFs for safeguards applications was considered during the May 2011 INMM Workshop Preparing for Nuclear Arms Reductions: Addressing Technical Transparency and Verification Challenges co-sponsored and facilitated by the Monterey Institute of International Studies. Analogous to certain arms control verification activities, some safeguards applications (for instance, in uranium enrichment facilities) may also require the special protection of sensitive or proprietary information acquired during analyses. The participants of the conference came to the conclusion that for progress in the nonproliferation and disarmament regime to continue, the arms control and nonproliferation community must recognize that a wide range of transparency and verification tools will be needed in the future, many of which may at this point be

---

[4] Luke, John S. "Exploring the Possibe Use of Information Barriers for Future Biological Weapons Verification Regimes", LLNL-SR-525091.

[5] Williams, Richard, et al. "Advances in Information Barrier Design". LANL, LA-UR-05-4149.

unknown or undeveloped.[6]

Brookhaven National Laboratory pioneered the IF field in the late 1980s with the CIVET concept. CIVET (Controlled Intrusiveness Verification Technology) was a proposed concept for arms control verification capable of using information while preserving its confidentiality in a bilateral environment.[7] Since the introduction of CIVET, there has been increasing interest in the expanded applicability of such concepts. However, the spectrum of possible techniques and the range of potential applications of the IF concept lack a unifying framework. This conservative paper-based scoping study seeks to illustrate reasonable options that could be pursued further as full-fledged research and development projects, if deemed necessary. Specifically this scoping study (1) surveys various IF techniques that have been proposed, developed and implemented; (2) identifies potential applications of IFs in a set of existing and future safeguards arrangements along with anticipated implementation challenges; (3) explores examples of IFs on the horizon and enhancements that might increase effectiveness; and (4) assesses and prioritizes the value to DOE of further efforts in this area.

An information barrier typically comprises a combination of hardware, software, and procedures/administrative controls that protect all sensitive information while providing non-sensitive results that are essential for the inspection mission and are trusted by both the monitoring party and the State/operator. The idea of an IF is conceptually simple: during an inspection, a measuring device (such as a gamma spectrometer) is protected within a system that includes an IF. The device measures the item under inspection, and the raw data feed directly into the IF. The IF serves to block (physically, and through data encryption) that data. It then provides a simple read-out to the inspector either supporting or negating that the material matches some predefined set of features.[7] This is often relayed through a green-light = “pass”, or red-light= “fail”, output. Figure 1 depicts a simplified schematic of the key features incorporated into an IF.

---

[6] Dreicer, Mona. “Report on the INMM workshop for Preparing for Nuclear Arms Reduction to Address Technical Transparency and Verification Issues”. INMM Annual Meeting, Palm Desert, 18 July 2011.

[7] Sastre, Cesar. CIVET: “A Controlled Intrusiveness Verification Technology”. Brookhaven National Laboratory, December 1988.

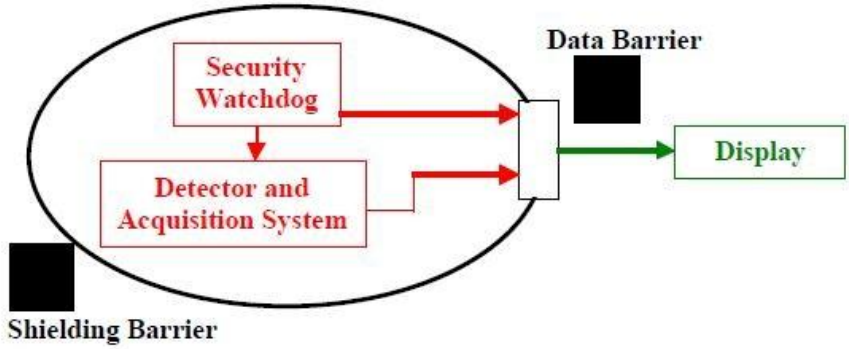

Figure 1: Simplified schematic of the main elements comprising an IF. The Detector, and Acquisition and Analysis System are physically-confined within a Shielding Barrier, which prevents direct visual/physical access to inspectors. The Data Barrier protects and obscures the sensitive data, so that only the attribute of interest is readable via the external Display. A Security Watchdog within the Shielding Barrier actively monitors this process, and automatically shunts the system by terminating all data collection if any threats, manipulations, or malfunctions are detected. (Figure adapted from Ref. 7)[8]

A key component of a successful IF is authentication - the process by which the monitoring party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item.[9] Varying perspectives have existed regarding successful authentication-in the early days of the Trilateral Initiative, 100% certainty was sought-while today a high degree of certainty would be considered useful and sufficient. It should also be noted that an IF is not a generic physical 'lock' that can be applied onto any measurement system in a plug-and-play fashion. IFs must be highly-tailored to the particular verification context under consideration, the detector, and the type of information needing protection. They also must be rigorously tested and 'red-teamed' to characterize performance, and assess any ramifications from potential inadvertent loss of sensitive data.[10] The results of such testing and analyses, once accepted by appropriate stakeholders, must absolutely precede inclusion of an IF in a real-life verification regime. Furthermore, IFs have to have a procedural component that includes the process of authentication and chain-of-custody, so that everyone has confidence in the hardware. Should the need for an encryption system become apparent in international safeguards, an IF with authentication, meeting agreed-upon standards, could provide a key tool.

---

[8] Fuller, J.L.; Wolford, J.K., "Information Barriers", IAEA-SM-367/17/01.
[9] Kouzes, R.T., W.K. Pitts, R.R. Hansen, "Introduction to Methods Demonstrations for Authentication". Pacific Northwest National Laboratory, PNNL-13941, July 2002.
[10] For a complete discussion on this concept, the reader is referred to Luke, John S., LLNL-SR-525091.

Terminology of Information Filters

In researching this paper, the authors have discovered that the more common term, 'information barriers', is reputed to have negative connotations in translation into other languages, especially Russian. This came up during the Trilateral Initiative work.[11] Apparently the connotation of the translation can be considered very negative in the Russian language, and has led to push-back solely on that basis in the past. In fact, other verification activities using the concept of information blocking have addressed this by using different terms. For example, for CTBTO activities, the term 'spectral blinding' is utilized. This also is not without controversy as some are confused about what is being 'blinded', the instrument or the inspector.[12] For that reason, the authors are suggesting the term 'information filters' herein.

a. How IFs have been used in the past

(1)Trilateral Initiative

The Trilateral Initiative was a multi-year effort involving the IAEA, the Russian Federation, and the United States. Throughout this project, all the players, including the IAEA, were concerned with the issue of authentication.[13] The goal of the Initiative was to investigate the legal, financial and technical issues associated with the verification by the IAEA of fissile material originating from defense programs. The Joint Working Group under the purview of the Trilateral Initiative developed concepts and hardware to address the needs of the Trilateral Initiative's verification mission, including IFs.[14] IFs were critical because the usual measurements that the IAEA makes – such as gamma spectroscopy – would reveal information considered by some sensitive in weapons-derived material. In fact, the development of IFs was a major aspect of the Trilateral Initiative.[15] The inclusion of IFs as a means to accomplishing the disarmament goals under the Trilateral Initiative served to underscore the potential impact IFs could have on arms control, disarmament, and nonproliferation.

Multiple efforts were undertaken to address the IF-type needs that the Trilateral Initiative highlighted. In 1999, the ISIB (Inspection System with Information Barrier) was demonstrated to a Russian delegation. The reason for the demonstration was to showcase the ability of the system to determine attributes of plutonium in sealed storage containers, and to show the feasibility of using an IF that protects sensitive information

---

[11] Correspondence with Michele Smith, May 2013.

[12] The term meant that the inspector was being blinded. Michele Smith, May 2013.

[13] Haas, Eckhard, Alexander Sukhanov, John Murphy, "Trilateral Initiative: IAEA authentication and National Certification of Verification Equipment for Facilities with Classified Forms of Fissile Material." IAEA SM-367/17/04

[14] Shea, Thomas E. "Report on the Trilateral Initiative: IAEA Verification of Weapon-Origina Material in the Russian Federation and the United States". IAEA Bulletin, 43/4/2001.

[15] Persbo, Andreas and David Cliff. "Verifying Warhead Dismantlement: Past, present, future". Vertic, delivered to UN ODA, 19 October 2010.

but nonetheless shows results that are meaningful to the verifying party and can provide a high degree of confidence.[16] The analysis of this system and its demonstration convey the following information regarding the use of IFs. First of all, the assessment of the demonstration noted that certain radiation measurements can be considered intrusive (for example, isotopic ratios). The information obtained from sensitive items or material can contain and potentially reveal sensitive information if subject to intrusive measurements. The IF addressed this situation by giving the host party assurance that sensitive information will not be revealed, while providing information that can allow for a verification conclusion.

As stated in the introduction, an IF typically comprises a combination of hardware, software, and procedures/administrative controls that protect all sensitive information while providing non-sensitive results that are essential for the inspection mission. The ISIF included a binary indicator (for example, of the presence of weapons-grade material).

The Trilateral Initiative involved the demonstration of an Inspection System with Information Barrier (ISIB). The particulars of the demonstration in 1999 included inspection of the attributes of plutonium in sealed containers without revealing sensitive information.[17] While the Trilateral Initiative dealt with weapons-grade plutonium as part of an arms control effort, the verification of nuclear material, stored in containers, and deemed sensitive by a host state, could easily be considered an international safeguards scenario, in which the same technologies could be applied. Managed Access can be used to block access to the material in the container in such a scenario, but the above scenario requires verifying the plutonium that is in the container based on more than solely visual recognition. Managed access includes physical shrouding types of barriers to protect some aspect of a physical object. This would not be as appropriate for aiding verification of data generated by some instrument measuring an object of interest. An IF would be a more appropriate solution by allowing such data to be verified in a protected manner (ex: encryption of raw data). Future safeguarding activities may include more intrusive verification activities, the sensitivities of which may not be comprehensively addressed by managed access alone (e.g., measurement of certain material at gas centrifuge enrichment plants, or verification of activities, data streams in a SILEX facility.)

The examination of the methodologies associated with the Trilateral Initiative underscored the U.S. contention that <u>certification</u> (of ability to protect sensitive information), and <u>authentication</u> (that the device is working as declared and would detect cheating) are complementary ideas, and both are critical in the development of IFs.[18]

---

[16] Luke, S.J. *et al*. "Verification of the Presence of Weapons-Quality Plutonium in Sealed Storage Containers for the Trilateral Initiative Demonstration". LLNL, IAEA-SM-367/17/08.

[17] Luke, S.J. *et al*. "Verification of the Presence of Weapons-Quality Plutonium in Sealed Storage Containers for the Trilateral Initiative Demonstration". LLNL, IAEA-SM-367/17/08.

[18] Luke, S.J. *et al*. "Verification of the Presence of Weapons-Quality Plutonium in Sealed Storage Containers for the Trilateral Initiative Demonstration". LLNL, IAEA-SM-367/17/08.

The Trilateral Initiative came to an early decision to define the verification and its scope such that that it could be politically acceptable while providing sufficient confidence and assurance as to the results of the disarmament activities under scrutiny. Although the technologies investigated during the Trilateral Initiative itself never passed the developmental stage, a 2002 Trilateral Initiative report concluded: [19]

The Working Group found no technical problem that would prevent the IAEA from undertaking a verification mission in relation to such fissile materials released from defense programs, and believes that many of the technical approaches could have broader applicability to other forms of fissile materials encountered in conjunction with nuclear arms reductions.

(2) CIVET

CIVET was envisioned as a tool to assist parties to an arms control treaty to verify each others' declarations with a sufficient degree of certainty. The theory behind CIVET was that "there is a significant difference between the information needed to verify the presence of nuclear warheads in a vehicle and the limited information that the various actors party to a treaty are willing or are legally able to disclose to each other."[20] CIVET was described metaphorically in terms of an inspector who could look at classified information based on which he would communicate a yes/no compliance answer to other members of the inspecting party, after which the memory of the inspector would be reliably erased. While the scenario was clearly fictitious, the underlying principle could be applied to a machine without any non-volatile memory. The theory was that if this were possible in a reliable and authenticated manner, the information provided by the communication of the "yes or no" would be acceptable to both parties.[21] Beyond the concept just outlined, a CIVET system was developed based on hardware composed of three parts: a sensor subsystem, a data processing and control hardware system, and a data processing and software subsystem. CIVET was designed not to require encryption. The functional hardware requirements and system requirements under consideration included:

1. Sensors- the sensor subsystem would be determined by the set of measurements needed for the verification of the issue in question. The choice of the sensors would be dictated by the type of material or system being verified.
2. Radiation detectors- These could be X-ray and/or gamma sensitive, and could be configured according to the mission's need. The choice would also be determined by the lowest technology compatible with the goals of the inspector.
3. Interrogation system- X-ray, gamma or neutron sources could be utilized if a level of uncertainty existed within the object to be measured, if exciting the target would assist with the output of results.

---

[19] final report of the Joint Working Group to the Trilateral Initiative Principals, from T.Shea, The Trilateral Initiative: A Model For The Future? ACT May 2008

[20] Sastre, Cesar. "CIVET: A Controlled Intrusiveness Verification Technology". Brookhaven National Laboratory, December 1988.

[21] Sastre, Cesar. CIVET: "A Controlled Intrusiveness Verification Technology". Brookhaven National Laboratory, December 1988.

4. Positioning devices- This could be accomplished using human ingenuity, or if necessary, more sophisticated systems, including robotic arms, etc. The need to change positions of the devices would need to be taken into account, i.e. using a robot or computer, if any other behavior would introduce a lack of certainty in the process.
5. A key aspect of CIVET as far as IFs are concerned was the signal conditioner, which would enlarge the signal sufficiently for it to be picked up by the detectors. A signal conditioner is key to the IF enterprise. CIVET's creators described the requirement of amplification, discrimination, pulse shaping, isolation and impedance matching of the output of radiation detectors.
6. Power supplies
7. Data processing and control- all functions of control should be performed by a computer.
8. Computer- There should be no hard disk, nor any components that could store information other than in a volatile memory. Software would be loaded directly before the verification measurements.
9. Data interface- The goal would be a simple interface that could be standardized across treaty verification efforts.

CIVET would require specified software in addition to the proscribed hardware. The output and reliability of CIVET is extremely dependent on the adequacy of the procedures associated with it.[22]

(3) The AVNG System

Scientists from the United States, Russian Federation, and the International Atomic Energy Agency (IAEA) created the initial AVNG system (*A*ttribute *V*erification System with an Information Barrier Utilizing *N*eutron Mutliplicity Counting and High-resolution *G*amma Spectrometry) during the Trilateral Initiative between the late 1990s-early 2000s. It used neutron counting and gamma spectroscopy to determine the presence of weapons-grade plutonium and the fact that the mass of plutonium exceeded an agreed threshold. These unclassified attributes must be determined by making measurements of classified parameters (i.e., the actual isotopics of the plutonium).

Figure 2 shows the three separate levels of containment provided by the system. The system included two measurement instruments, a neutron multiplicity counter and a high-resolution gamma ray spectrometer. The physical barrier hindered direct tampering with the system. Software was minimized and installed in a read-only format (cannot be modified) to increase data protection. Another feature providing an extra level of security centered on the "security watchdog" element (in purple, Figure 2).

[22] Sastre, Cesar. CIVET: "A Controlled Intrusiveness Verification Technology". Brookhaven National Laboratory, December 1988.

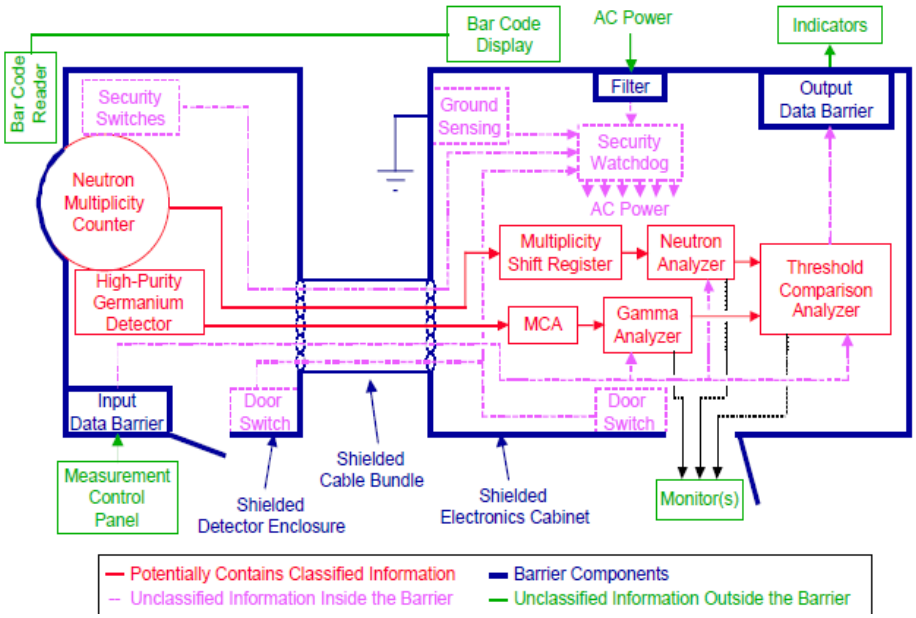

Figure 2. The AVNG system including an Information Barrier (in blue) to protect sensitive data produced by a neutron multiplicity counter and a gamma spectrometer (in red).[23]

This element remained separate from the measuring devices, and disconnected AC power to all components if internal ground sensors detect any attempts to tamper with or break open the system. On killing the power, all measured data obtained to that point would be erased, as it was stored solely within "volatile" memory (i.e. not stored to the computer's long-term memory). A challenge of particular import that the AVNG team addressed was the need to select measurement methods in which unclassified calibration standards could be used as a basis for measuring classified material. Testing with such unclassified reference materials is one means to provide the inspector with some degree of trust in the functioning of the device.[24]

Because of these strengths the AVNG seems an excellent choice for consideration within a safeguards context where classified or sensitive isotopics are of concern. However, the earliest system did include some inherent drawbacks. For instance, the system was not appreciably portable (early prototypes had a footprint roughly the size of a refrigerator). The system also needed a large pool of reference data (from measurement of unclassified reference materials) to authenticate the data produced and to give all parties confidence that it would measure classified materials correctly.[25] AVNG scientists mentioned the difficulty in obtaining appropriate numbers and types of reference standards that would closely enough resemble the classified

---

[23] Figure adapted from: Langner, Diana G. *et al.* "Attribute Verification Systems with Information Barriers for Classified Forms of Plutonium in the Trilateral Initiative". LANL, LLNL, IAEA, RFNC-VNIEFF, IPPE. IAEA-SM-367/17/02

[24] Ibid.

[25] R. T. Kouzes, C. Pura, L. Bratcher, A. Riedy, et al., "Authentication Procedures – The Procedures and Integration Working Group", July 2001, PNNL-13550.

components of nuclear weapons.[26] The system also performed in two modes: open-mode (for diagnostic/non-classified measurements) and secure-mode (for classified measurements). If the system malfunctioned during an inspection (in secure-mode), the inspector likely could not perform diagnostics to uncover the malfunction- the system would only indicate the system's performance as "OK" or "NOT OK". Only in the open-mode could diagnostic information be obtained (after a period of time, by the host). AVNG scientists also cited this as one area needing further research and development, in order to make the system as rapid and robust as other instruments routinely used in IAEA-type inspections of nuclear materials. Subsequent AVNG systems sought to address these challenges.

The AVNG system was demonstrated at Sarov (VNIIEF) as part of the Trilateral Initiative in 1999, and performed as expected. The only issue with this demonstration was that the U.S. participants were not permitted access to the facility where the demonstration was to takeplace, due to lack of necessary clearances for foreign visitors. While the U.S. representatives could not physically observe the demonstration on-site, the parties reached a compromise by videotaping the activities. The U.S. representatives from an off-site location periodically called the site at a noted time throughout the demonstration and asked their counterparts to perform certain visible tasks in front of the camera. This gave confidence to the U.S. observers that the demonstration on tape was not pre-recorded.[27]

It should be noted that this challenge was not instrument- or process-based. Indeed, the AVNG went through the certification process at that facility,demonstrating the operators' confidence in its efficacy. The observers' confidence in the IF, despite their remote location during the demonstration, was also high.

The challenge faced during this AVNG demonstration was specific to the unique security environment for a nuclear facility in the host country; a NWS. In an IAEA safeguards inspection scenario, in a NNWS facility, the likelihood of facing a similar challenge would be slim.

(4) CWC Onsite Inspections

The Chemical Weapons Convention (CWC) verification regime does allow for a simple IF methodology for masking sensitive, and/or confidential, proprietary Information (CPI) during CWC onsite inspections. This falls under a set of CWC managed access procedures allowable during routine and challenge inspections- procedures which bear similarities to some of those associated with safeguards managed access. Specifically, inspected CWC Parties have the right to:

"…take measures to protect sensitive installations and prevent disclosure of confidential information and data not related to chemical weapons. Such measures may include, inter

---

[26] Langner, et al. "Attribute Verification System with Information Barriers for Classified Forms of Plutonium in the Trilateral Initiative", IAEA-SM-367/17/02.

[27] Kondratov, Sergey *et al*. "AVNG System Demonstration". Proceedings of the 51st Annual Meeting of the Institute for Nuclear Materials Management.

alia: […] ***Restriction of sample analysis to presence and absence of chemicals*** *listed in Schedules 1, 2 and 3 or appropriate degradation products;"*[28]

It is worth noting that commercial, civilian chemical industries are primary sites subject to inspection under the CWC. One might argue these inspectees bear similarities to the types of inspectees (civilian nuclear sites and industries) subject to inspection under IAEA safeguards. An IF is allowable under CWC inspections to provide a confirmatory yes/no answer with regard to the presence or absence of CWC Scheduled chemicals. This high-level, confirmatory-only kind of granularity is all that is needed to meet Treaty obligations. The fact that IFs protect CPI while meeting treaty obligations under the CWC verification regime, along with their use in masking data in enrichment plants, suggests that their expanded use in other safeguards contexts should be palatable to the IAEA and other safeguards stakeholders.

3. Current Generation Information Filters: The AVNG 2.0

An important set of questions needs to be explored before we can investigate potential challenges and/or opportunities presented in possible application of an IF to any safeguarding activities. This set of questions centers on the current state of the art technology for IFs currently being pursued in the arms control verification realm; what lesson can we learn from years' of research and refinement to develop this improved system?; what improvements did they make and why? Finally, are there any indications of challenges to implementing this new system in a real-life context, for example, in support of any current/future verification regime? Armed with some of this information, we may better address or predict likely challenges we may face in our safeguarding context. We can't ignore the fact that the challenges presented by implementing an IF in a multilateral safeguards context may be even greater than those presented in the bilateral arms control verification context; simply put, there are more stakeholders to satisfy. One of the challenges of using such a tool in a multilateral environment is getting all the parties to agree to use the tool in the first place. This includes not only Member State approval, but also the approval of the IAEA Secretariat itself. Verification of activities related to civilian, peaceful uses of nuclear technology stand at the heart of IAEA safeguards – this is a very different situation than the supremely sensitive act of verifying nuclear weapons-related activities under arms control verification regimes.

AVNG: Current Status

The Trilateral and initial AVNG work has been followed by continued USG support resulting in further demonstrations and prototypes,[29] including:

- The Fissile Material Transparency Technology Demonstration. This took place at LANL in 2000 with Russian presence; its objective was to demonstrate the

[28] Chemical Weapons Convention Bulletin, Department of Commerce Bureau of Industry and Security, Publication CWC-010, updated May 2006. The bold and italics added by authors for emphasis.

[29] Review of Prior U.S. Attribute Measurement Systems, Greg White, INMM, July 2010

acquisition of six unclassified attributes behind an IF.

- Support for a Russian AVNG prototype. A Russian demonstration took place at Sarov in 2009 with U.S. presence and demonstrated the acquisition of three unclassified attributes. [30] This work was funded under NA-24's WSSX subprogram.
- The Next Generation Attribute Measurement System. This program lasted from 2005 to 2008; the purpose was to use commercial off-the-shelf components. While this has advantages in terms of cost, development time, and reliability, it made authentication more difficult.
- A third-generation attribute measurement system is under development which is intended to "… further the scope of previous systems by including additional attributes and more rigor in authentication."[31]

The ideal AVNG would include three important characteristics. It would be 1) be highly reliable, 2) "certified" by the inspected party to be acceptable to operate in a classified environment on its classified items, and 3) "authenticated" by an inspecting party so that the inspectorate is assured the device operates as declared. Satisfying all three of these conditions with a complicated device that incorporates both neutron multiplicity counting and gamma spectrometry (as all these devices must to measure an attribute like plutonium mass) is a tall order: design choices that achieve one objective tend to make the others harder. While the initial Trilateral technical work was reported as a success, "… the system was neither certified by the U.S. for use on sensitive items, nor authenticated."[32] And while much progress has been made subsequently, especially in the areas of certification and reliability, it is probably fair to say that at the time of this writing one cannot point to a system that demonstrates all three characteristics. The issue of authentication will certainly need to be addressed for a system to be adopted by the IAEA.

B. The Norway-UK Initiative

The Norway-UK Initiative was a cooperative project examining the verification techniques and procedures that would be required for hypothetical disarmament verification between a nuclear weapons state (NWS) and a non-nuclear weapons state (NNWS). The states in the initiative, played by the UK and Norway, were fictitious, with actual roles reversed; i.e., Norway played the role of a NWS and the UK the role of a NNWS. The operation relied heavily on improving trust and confidence between the two parties, and attempted to address both political and technical challenges underpinning a disarmament regime.

The project produced multiple reports, including one specifically dedicated to the issue of IFs as a tool for verification. The report noted "In a future verification regime for nuclear warhead dismantlement, inspecting parties are likely to request measurements on warhead and warhead components, to ensure that the items presented are consistent with

---

[30] Kondratov, S., *et al.*, "AVNG System Demonstration," Proceedings of the 51st INMM Annual Meeting, Baltimore, MD, July 2010.
[31] Review of Prior U.S. Attribute Measurement Systems, Greg White, INMM, July 2010
[32] Ibid.

the declarations made by the host party. Such measurements are likely to be based on radiation signatures, and would be used to confirm physical attributes of the fissile material present within the system. Almost any measurement of this type, which would be of use for inspection purposes, would be likely to contain sensitive or proliferation information. It {was} therefore essential for such measurements to be performed behind an information barrier which, while protecting the [data would] reveal a pass/fail to an agreed attribute threshold." The project noted, going beyond purely technical details of obscuring or sanitizing information, "…that the information barrier design process builds in mechanisms whereby both parties can have high confidence in the validity and veracity of any result obtained."[33]

Although this study is a bilateral example of IF cooperation for disarmament, it could be relevant to multilateral safeguards implementation of IFs. For example, the IF prototype 1 that the report described is designed to detect the presence of a given radioisotope. The type of nuclear material(s) present would be determined by the presence of peaks in a high-resolution gamma spectrum.[34]

5. Potential Application of the IF Concept in International Safeguards

General Challenges

Intrusiveness concerns are not foreign to the world of safeguards activities, such as inspections under managed/complimentary access, etc. Just as an arms control verifier from a NNWS could discover sensitive and/or CPI under the NPT in a disarmament scenario, so too could an IAEA inspector from a NNWS, inspecting a facility under a comprehensive safeguards agreement (CSA) or AP. The challenges to international safeguards are potentially even greater in regards to protecting information, as instead of simply two parties inspecting each other, the numbers of states and approvals involved will be much greater.

International safeguards now functions largely without the need for IFs for two reasons: safeguards are for the most part applied to the civil nuclear cycle, where materials and processes are largely free of highly-sensitive information; and where there are sensitivities, INFCIRC/153 (paragraphs 4, 5, and 8) provides for a confidentiality regime to protect sensitive information acquired by inspectors. However, there are some exceptions to these conditions.

Some civil facilities (e.g., centrifuge plants) contain highly sensitive technology, and it may well be that newer technologies (e.g., pyroprocessing, SILEX) will provide more such examples.

---

[33] Chambers, David M, *et al*. "UK-Norway Initiative: Research into Information Barriers to allow warhead attribute verification without release of sensitive or proliferation information". AWE (UK), Institute for Energy Technology (Norway), Norwegian Defence Research Establishment. 2010.

[34] *Ibid.*

Some safeguards activities are carried out in states that have nuclear weapons – and those situations will increase if the IAEA takes on responsibilities beyond the NPT (i.e., FMCT, plutonium disposition).

Despite the IAEA's confidentiality regime, states and operators may make claims that some information needs to be withheld from inspectors for national security or business confidentiality reasons, and the IAEA may not always able to dismiss such claims in negotiations. These exceptional situations, along with those listed above, could warrant application of IFs. Furthermore, a number of examples where IFs might find application in safeguards are listed below.

A. Verification of Enrichment Plants

DOE has placed a high priority on effective international safeguards at enrichment plants; procedures must address both diversion and misuse. Remotely monitored in-plant sensors that gather large amounts of operational data are one way to do this effectively and efficiently. However, these facilities also must protect sensitive technology, and are part of an internationally competitive business. The conflicts between these objectives have been manifest since the Hexapartite Safeguards Project in the 1980's and continue to this day. URENCO is not reticent about its need to protect its information: "… the safeguards verification regime has to be designed well, to avoid disclosure of sensitive information and technology: URENCO does not want its competitors to know what it is doing and especially URENCO does not want to help potential proliferators."[35] URENCO wields considerable influence in this area, and generally expresses reluctance to provide detailed operational data (even if it is not proliferation sensitive) on the grounds of business confidentiality. All this suggests a role for information barriers in advanced enrichment plant safeguards; three examples follow.

I. Use of IFs for in-line sensors on process piping. Some applications have already been developed, although they are no longer in use: the CHEM and CEMO systems were for a time employed in URENCO facilities to monitor enrichment levels in header piping – they produced only YES-NO indicators of higher-than-declared enrichment levels. While the IAEA now uses environmental sampling to detect HEU production, this technique has drawbacks and may not be universally applicable. For example, one reason for this is that certain NWS do not allow environmental sampling, citing a national security exemption. While the actual enrichment levels are not proliferation sensitive, they may be regarded as sensitive from a business standpoint; moreover, cascade gas pressures on which the enrichment value is based may be classified. While enrichers seem to have "little enthusiasm" for current devices, they do not seem to be unalterably opposed to improved versions the concept.[36]

II. Use of IFs associated with sensors in feed and withdrawal operations. The IAEA could continuously monitor cylinders on feed and withdrawal stations using load

---

[35] URENCO'S VIEWS ON INTERNATIONAL SAFEGUARDS INSPECTION, Peter Friend, 8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR.

[36] URENCO Conference on GCEP Safeguards, held in December 2009, Peter Friend, IAEA-CN-184/210.

cells. It could also monitor accountability scales. This would provide very strong monitoring of the material balance around the cascade; it might save considerable inspector effort measuring UF_6 cylinders. This is detailed proprietary operational data that operators like URENCO are not inclined to agree to release. An IF could address the operators' concerns that a continuous stream of proprietary data was observable in a safeguards activity. One way this could function would be that a simple green/red signal output of the IF would demonstrated that a continuously monitored and obfuscated raw data stream, was within pre-set specifications. The IF would display red only if an out-of-specification activity were to occur in the process being continuously monitored and filtered. Thus, the system is allowing safeguards verification activities, while addressing any operator concerns with regard to unrelated sensitive data being released to an inspector.

III. Safeguards for a SILEX enrichment facility (and other advanced sensitive facilities). Such a facility is being developed by the United States based on Australian technology. Making this civil nuclear facility available for selection for safeguards will necessitate a safeguards approach that does not divulge Sensitive Nuclear Technology. As SILEX is a civilian technology, if a facility is constructed, it will have to be offered for IAEA safeguards under the U.S. Voluntary Offer. The design of the facility appears to very closely-held.[37] Little is publically-available about the details of the technology, but it seems clear that much of it will be sensitive. Under these conditions it is not possible to provide specific suggestions as to what sensors will be needed for SILEX safeguards, but it seems very likely that information protection will be major concern, and therefore IFs will almost surely have to be considered. More generally, for future advanced facilities in which safeguards are built-in "by design," there is the potential for large amounts of data-sharing with the IAEA. Some of this data may be considered sensitive by the operator, so there may be a need for incorporation of IFs as an element of "safeguards by design."

B. Complementary Access Inspections, Additional Protocol

The implementation of the AP, and associated complementary access (CA) visits, is an area with demonstrated needs for an IF-like technology. CA inspections are an IAEA inspection mechanism under the Additional Protocol. They allow the IAEA rights to inspect certain locations in a State, under a mutually-agreed upon set of procedures.[38] A CA inspection generally seeks to meet one or more of the following objectives: 1) to assure absence of undeclared nuclear materials or activities, 2) to resolve questions or inconsistencies with respect to declarations under Article 2, and/or 3) to confirm decommissioned status of facilities and locations outside facilities.[39] CA inspectors

[37] Enrichment Separative Capacity for SILEX, John Lyman, LA-UR-05-3786 (this appears to be part of POTAS project).

[38] Cited directly from International Nonproliferation Safeguards Engagement Program reference document on CA, Ch. 6, obtained courtesy of BNL INSEP lab support team members.

[39] INFCIRC/540

usually carry a toolkit to perform necessary measurements within the inspected facility to achieve these objectives. The CA toolkit currently consists of simple measuring devices such as a voice recorder, GPS device, a camera, and a hand-held gamma detector, the HM-5 (Figure 3).

Figure 3. Typical IAEA CA toolkit with hand-held gamma detector (HM-5), voice recorder, GPS, camera labeled.

The HM-5 is the only existing toolkit device that measures nuclear properties (specifically, the gamma spectral signature) of nuclear materials (Pu, unshielded U).[40] It is an accepted IAEA device already routinely used in the field on CA missions. This device is not expected to warrant retro-fitting with an IF, as data obscuring features have not been explicitly requested by stakeholders.

However, one current activity of interest to the IAEA, and the Next Generation Safeguard Initiative's (NGSI's) Safeguards Technology program, is the investigation of other portable COTS technologies that might expand and enhance the IAEA CA toolkit. This is because as the IAEA moves away from a traditional measurement-based safeguards approach to a State-Level Concept, the importance of detection of undeclared activities (especially through extant IAEA mechanisms like CA) is heightened. Beginning in FY13, the Complementary Access Working Group (CAWG), a multi-laboratory team comprising experts from BNL, INL, LANL, and SNL, was established. The CAWG's four-phased, multi-year project consists of performing a technically sound, systematic and comprehensive investigation of potential observables for nuclear fuel cycle activities and facilities to determine which are of greatest interest from the perspective of CA and identification of ready or near-ready COTS to detect such

[40] The IAEA does have an extended set of instruments they may use in special CA circumstances; recorded by Verdugo, Feb 2013 from meetings with IAEA representatives, Complementary Access Working Group Study.

signatures under a CA regime.[41] As radiation-measuring devices are well-established systems already in place and being further investigated by the IAEA, the CAWG is focusing investigations on multifunctional chemical-detecting COTS technologies that could be readily-adapted to, or customized for practical inspector use.

The technologies under consideration, including (but not limited to) Mass Spectrometry, Raman Spectroscopy, and X-Ray Fluorescence all present opportunities for a much larger set of fuel cycle indicators detectable on a CA mission. Implicit in this, however, resides a potentially unprecedented level of intrusiveness, as these systems can provide a high-level of certain quantitative data during analyses (for instance, isotopic ratios, concentrations, sample purities and compositions, etc). For instance, as mentioned in a previous section, GCEP operators consider certain processes and data streams proprietary. These chemical detection techniques under consideration can adequately measure the exact chemical composition of many of these proprietary data streams, for instance revealing enrichment levels, concentrations of actinides (plutonium and uranium), and any chemical impurities or contaminants in the process. Consideration of IF inclusion into the CAWG's proposed COTS is outside of the scope of work for that project. However, in a joint IAEA-NGSI-CAWG kick-off meeting in Feb 2013, IAEA representatives noted interest in investigating the possibility of 'switching' proposed COTS technologies between a high-resolution data depiction mode (such as a gamma spectroscopy read-out) and a low-resolution "yes/no" mode (such as a simple "green/red" light read-out)[42]. The instruments that are under consideration are created in order to be maximally intrusive. This intrusiveness level, while sought for some applications, such as chemical/biological warfare agent detection and forensics, could be problematic for CA applications. For chem/bio applications, a premium is put on detecting and recording as much chemical information as possible, as opposed to in the CA environment where intrusiveness must be balanced with information protection. For instance, the detection of explosives indicators would be of value on a CA mission (to discriminate between legitimate industrial uses and undeclared activities). However the IAEA would need to carefully handle classification/sensitivities issues if these indicators were detected.[43] Inclusion of an IF could potentially address this future challenge. 'Information obscuring' or filtering has likely not been a priority for manufacturers of these instruments. Determining whether they could be modified to simply alert to the presence or absence of an indicator is something the CAWG could explore. While that demonstration would fall under the purview of the CAWG, for the purposes of this study, the authors note that there is a safeguards/CA research project where inclusion of an IF could be tested.

---

[41] One of the authors of this study is a BNL participant in the CAWG.

[42] The terms utilized by the CAWG IAEA representatives were "high-resolution quantitative" versus "low-resolution qualitative" switching modes for an instrument.

[43] These comments are paraphrased from notes captured in the meeting's After Action Report.

C. IAEA's expanding role in arms control: the FMCT[44]

In the event that the Fissile Material Cutoff Treaty (FMCT) includes verification provisions to be implemented by the IAEA, IFs developed for safeguards could play another role by being re-purposed for FMCT verification. The possibility of overlapping safeguards and arms control measures is not new. However, IFs have historically been considered solely an arms control measure. Utilizing such technologies for multiple purposes could present cost-savings for each verification regime, such as international safeguards via the IAEA, and for domestic inspections or regional agreement verifications. They could also increase transparency, strengthen assurances during both inspections and verification activities, and present a heightened level of protection for nuclear materials, technologies, facilities and processes.

Whereas NPT safeguards focuses on the NNWS, the FMCT would surely involve inspections in many locations (either at declared facilities or undeclared sites) in NWSs and other nuclear weapon possessors that are associated with sensitive information (either sensitive nuclear processing information, or weapons-related information). The possessor states are more secrecy-driven and less acquainted with intrusive inspections than the NNWS. An FMCT would therefore push the concept of "safeguards" into situations where the conflict between verification and protection of sensitive information is more acute. IFs could therefore be expected to play a larger role in FMCT verification than in conventional safeguards.

6. Anticipated Implementation Concerns with IFs for Safeguards

Facilities and the IAEA may have concerns, including: How the introduction of this technology will affect their movements and operations, and how effective IFs will be in protecting sensitive information. These concerns will have to be mitigated on a case-by-case basis, by addressing the need to balance intrusiveness and sensitivity, and by finding a fulcrum between high-confidence for inspectors and abiding by the NPT, etc.

Table 1 outlines the technologies and procedures the paper has examined, and plots the activity, sensitivity issues, describes the challenges that would be met, and predicts the level of difficulty in implementation.

Table: Comparative challenges that IFs could address

Safeguards	Potential	Would an	Predicted level of	Recommendation	Value Judgment for

[44] According to the Statute, any verification the Agency undertakes is considered safeguards.

Activity	Information Sensitivities	IF meet a currently unmet challenge?	difficulty in implementing an IF		Recommendation
Verification of enrichment plant technologies	Enrichment levels	Maybe	Difficult since plants already designed, would have to include design parameters for post-fabrication implementation	Targeted study of verification for E.P.s needed	The authors believe this case warrants a more in-depth study on where/when/how an IF may be introduced into an already designed plant in order to determine whether this would be feasible and/or would meet an unmet safeguards need.
Detection of HEU production (CEMO)	Cascade technology parameters	Yes	Depends on plant design	Targeted study of verification for CEMO could be useful in making determination	
SILEX	Technology system itself and enrichment data	Maybe	Not enough information about SILEX to predict	In the authors' opinion further information regarding the sensitivities involved with SILEX is necessary before making any near-term decision as to the feasibility of IF inclusion.	Much about SILEX is sensitive (the technology and data), The authors reason that IFs might be a means to protect the data. For the technology, Managed Access may be more appropriate means of protection.
Managed Access	Already captured by physical protection means (ex: shrouding, masking)	No	N/A	No action.	Managed Access is a complementary, separate means of physically protecting information.
Complementary Access	Quantitative nuclear, elemental, or chemical signatures (if new chemical COTS becomes part of CA toolkit)	Perhaps, for future challenges if new COTS technologies introduced to expand CA toolkit.	Moderate difficulty- could build-in to consideration of any new chemical COTS technologies prior to implementation	The authors' recommend sharing their findings with the CAWG to determine if an IF could be tested in conjunction with COTS technologies under consideration.	The authors base their recommendation on 1) noted interest from the IAEA in potential data obscuring during CA, and 2) the ease with which a simple IF demonstration may be added to the forthcoming COTS technologies testing campaign.

Table 1. A comparison of the different safeguards applications assessed, type of data warranting protection, and likelihood of appropriateness in suggesting use of an IF.

7. Safeguards challenges that could be addressed with IFs

Table 1 charted a preliminary set of safeguards activities that might benefit from inclusion of an IF. This list of potential IF candidates while not exhaustive, can be further characterized into the following three categories:

Existing safeguards challenges that could be addressed with IFs

a. Verification of enrichment plant technologies
b. Detection of HEU production (CEMO)

The authors suggest that a near-term, targeted study for either/both of these activities in order to determine whether IFs would be useful (e.g. for protecting enrichment level information during an inspection). The authors note that such studies would benefit from a detailed cost/benefit analysis, since plants are already designed and would need to be modified to include any new data obscuring/encrypting technologies. It may be determined that protecting information via IFs in already-designed systems is not the best strategy. Validation and/or re-certification of these plants using IFs would likely be a difficult, costly task. Operators and IAEA stakeholders would need to be brought into this discussion for a realistic assessment.

Foreseeable safeguards challenges that might be addressed with IFs

c. SILEX
d. Complementary Access

Both the technology and data generated in the SILEX process are so sensitive that it is difficult to fully predict whether an IF feature would be beneficial. Likewise, it is difficult to predict what safeguarding challenges/activities will take place in such facilities. Because of the current opacity surrounding SILEX, the authors deem it premature to suggest for IF investigation.

Complementary Access, however, does seem like an interesting, timely case for further consideration. This is because the IAEA is currently considering expanding their CA toolkit to include potentially intrusive COTS chemical detection technologies (chemical counterparts to the HM-5). Some of the technologies under consideration are used elsewhere for chemical forensics and trace environmental sampling. These technologies have the capacity to collect or reveal a wide range of signatures outside of the scope of a CA inspection. The authors' reason that there is value in a near-term study to fully-scope whether introducing these enhanced detection tools raises any sensitivities from an operator's and/or inspector's perspective.

Finally, not included in Table 1, but of interest for the anticipated role that IAEA the IAEA may play, is the case of the FMCT. FMCT verification will not be a safeguards issue directly, but any verification activities of such a treaty may fall under the IAEA's purview. A placeholder should exist for potential FMCT-related verification challenges that IFs could address for the IAEA.

8. Next steps and recommendations

In order for the application of IFs to be palatable and seen as an attractive option by the IAEA, the problems posed by a lack of authentication and certification needs to be addressed. The IAEA should be able to have a high degree of confidence that the instrument will be able to not only detect but also authenticate. A weakness of current work to date is that authentication has not been the focus; most of the work has focused on getting a prototype working, or certifying that no sensitive information will be disclosed. While considerable effort has been directed toward addressing concerns about authentication under the Trilateral Initiative, further study on authentication could be beneficial. One recommendation is to review the work that has been done in arms control on IFs and determine if the existing authentication standards (1) are adequate; and (2) would they satisfy potential IAEA safeguards needs. If the answer is other than affirmative, one conservative recommendation is to provide follow-on analysis and reporting.

Prior to any further consideration of IFs for specific safeguards applications, any issues with terminology associated with the act of information filtering should be addressed. As mentioned earlier, the Trilateral Initiative activities uncovered unanticipated concerns with the term "information barriers", as this could be seen to have negative connotations when translated into the Russian language. The authors recognize the need to find an innocuous term to use instead of information barriers that would be acceptable in the international safeguards environment.

Another finding and consequent recommendation is to engage the IAEA to consider whether any potential IF application for safeguards could assist inspectors. For instance, could an IF enable them to better monitor specific process points, or allow them to obtain more information from the operator than they are currently able to obtain.

This paper mentioned CEMO, enrichment plants, SILEX and CA tools as existing/foreseeable safeguards challenges that could be addressed with IFs. These areas could benefit from more in-depth, targeted analysis. Once such analyses have been undertaken, the process of developing IFs for safeguards will be closer to the point at which research and development plans may become reasonable and have visible, near-term applicability and utility.

The authors recognize that adding any new technology to the suite of analytical instruments approved for use by the IAEA for safeguards activities is likely to be challenging. The IAEA must revise, extend, or annex existing agreements to include new technology additions; this will undoubtedly be a time-consuming process involving many stakeholders. There may also be a need to assess any concerns over IF terminologies, definitions, or processes borrowed from arms control contexts. A rebranding strategy to better reflect safeguards applications could be a useful endeavor. To meet future safeguards demands, new approaches to verifying and protecting certain information collected on an inspection would benefit all IAEA safeguards stakeholders, and support the Agency's key obligation to verify peaceful uses of nuclear materials. Table 1 summarized the selection of safeguards activities considered in this scoping study that might/might not benefit from inclusion of an IF. We ruled out the appropriateness of an IF for safeguards managed access activities since information is already being obscured by other physical means.

The authors have highlighted an FY13 NGSI-funded multi-year working group investigating chemical COTS technologies to enhance the CA toolkit. That group is currently in Phase 2 of their study, performing a systematic analysis of portable, multifunctional technologies that could be readily-adapted to, or customized, for practical inspector use. Phase 3, expected to be initiated in FY14, will entail purchase of candidate COTS equipment, a detailed test plan for assessing functional and performance specifications, and a rigorous testing phase for each instrument.[45] This presents a timely, unique opportunity to maximize the results from that effort.

One recommendation, as a follow-on IFs for safeguards study, could consider whether a simplified IF could be integrated into the chemical COTS instruments already under investigation seems like a cost-effective leveraging opportunity for two NGSI teams. The authors of this study suggest reaching out to that group, learning from their functional and performance specification testing campaigns, and exploring ways that an IF might augment (or diminish) performance in the field. The authors here could develop a mock CA inspection scenario to add in their testing campaign, where the possibility of 'switching' instrument outputs between a "high-resolution quantitative" mode and a "lower-resolution qualitative" one could be analyzed. As noted earlier, this capability is something of interest to the IAEA.

Gas centrifuge enrichment plants have overlapping verification points, where both safeguards data and proprietary facility operator data can be extracted. The specific challenge identified is the detection of undeclared feed in GCEP in the form of excess LEU production. The reason that this is a safeguards need that could have data filter relevance is that some GCEP operators, such as URENCO, are unwilling to share data obtained from continuous monitoring of load cell data due to issues of sensitivity and/or proprietary information, yet clearly the IAEA requires a complete understanding of GCEP operations and feed in order to successfully verify/implement safeguards at a plant. While the IAEA has the ability to use environmental sampling and Limited Frequency Unannounced Access to verify certain aspects of GCEP operations, and to have access to cascade halls, these tools are not sufficient in determining that no excess LEU production is occurring at a facility. This study recommends undertaking further research directly relevant to the challenges and needs posed by GCEP relevant to international nuclear safeguards.

[45] CAWG FY13 Proposal (BNL, LANL, INL, SNL).