INFORMATION PROTECTION WHEN APPLYING SAFEGUARDS TO CENTRIFUGE ENRICHMENT FACILITIES

Orpet J.M. Peixoto
ABACC- Brazilian Argentine Agency for Accounting and Control of Nuclear Materials
Av. Rio Branco 123 Gr 515, 20040-005-Rio de Janeiro- Brazil
E-mail : orpet@abacc.org.br
Laércio A. Vinhas
CNEN – Nuclear Energy National Commission
Av. Rua General Severiano 90, CEP 22290-901-Rio de Janeiro- Brazil
E-mail : lavinhas@cnen.gov.br

I - ABSTRACT

The application of safeguards in sensitive installations is always a balanced task where the safeguards organization must accomplish their safeguards objectives and at the same time to avoid accessing unnecessary information which may be used in proliferation activity.

On the other side the installation owner wants to protect what he considers to be sensitive or commercial information. Usually the protective control measures introduced by the plant operators make the safeguards activities more complex and requiring more safeguards effort in order to fulfill the safeguards objectives.

The safeguard approach currently applied for commercial centrifuge enrichment facilities are based on the Hexapartite Project, which during its development took the information protection in consideration. However in some plants, due to special requirements, the Hexapartite control measures can not fully applied and other specific alternatives control measures shall be implemented.

The paper discusses the hole of sensitive information protection based on non-proliferation issues, disclosing of technological and commercial information and also on some state owner political concerns. A concise analysis on information protection taking into account the safeguards approaches and activities, the inspection effort and the plant profile is presented. The paper also suggests points to be considered by agencies and plant owner in order to have an information protection balanced safeguards approach.

II - INFORMATION PROTECTION

To preserve information data will be always a crucial matter for any country, company or human relationship in any life activity. The success of a political issue, a military operation, a commercial contract or even an in house protection system will depend upon how the counterpart, or adversary, has access the information on the matter (process) that is going on. To obtain and to protect the information is also a basic activity for many states, companies or persons related with the success of the well manage situation. There is a large the number of systems and organizations in the world specialized in information managing and also inside the organizations there are structured branches dedicated only for information treatment.

This is not different in the nuclear field. To make the things a little more complex, in some activities, as such nuclear, chemical, biological, where the information can contribute to Production of Weapons of Mass Destruction (WMD), the risk on proliferation is a major concern. In these cases the information protection poses an additional task, because the proprietary owner deals with the secure of information not only for their own success but also to avoid the proliferation by the ones that will have access to the information, which implies in denying to the counterpart the possibility of proliferation and avoiding being charged with the responsibility for allowing the spread of the information.

Procedures for handling the various categories of sensitive classified or unclassified information vary from one State to another. This is due to different legal and/or regulatory

requirements for each category and the State or organization's implementation of those requirements. Information classification as sensitive classified or not, is also important. The answer to the question - **Which information needs to be protected? –** will determine the information sensitive and how much care we must have to manage it.

Which information needs to be protected? An analysis methodology.

In order to find which information in a system needs to be protected, one should submit the system (process) to the factors analysis listed below, such as:

- Degree of information sensitivity: First identifies what is sensitive or critical information. That means, what we are trying to protect. Look the real importance of a set of data relating to my process bearing in mind if; it will influence my goals in case of disclosing (acquisition, timing, technology, etc); or, it will allow the counterpart to reach objectives that are internationally denied (proliferation); and/or it will be commercially prejudicial to the organization/country. Is this information in the public domain or can be obtained in open source literature;
- Nature of the threat to the information: The analysis of the threat leads to determine who wants or needs our critical information and how our adversary might collect our information. We analyze the potential application of our data, along with the flow of information, to ascertain which adversary would be interested in what data, and how he would be able to obtain them. In safeguards one may consider the inspectorate organization as sympathizer or someone who supplies data to the active adversary.
- Vulnerability of the information: In this phase we look at vulnerabilities, direct and indirect, surrounding the process operation. We look at how the activity actually works, rather than how people think it works, identifying the points where the sensitive technical or commercial information can be obtained. We consider the magnitude of the vulnerabilities combining the information sensitivity and the weakness of the information protection tools. The situation of inadvertent release, when someone who accidentally gives away information is also taken in consideration;
- How to protect the information: Countermeasures, finally, are the solutions that a manager employs to reduce risks to an acceptable level, whether by eliminating indicators or vulnerabilities, disrupting the effective collection of information, or by preventing the adversary from accurately interpreting the data. Countermeasures are dictated by cost, timing, feasibility, and the imagination of the personnel involved. The most effective tend to be simple, straightforward, and inexpensive procedural adjustments that fit the solution to the need. Countermeasures are instituted in rank order to protect the vulnerabilities having the most impact. Multiple countermeasures, enacted together, often provide a synergistic effect that compounds the benefits without unduly raising the cost level.

At this stage, the manager evaluates the risk to his or her operation or activity, asking: "Does the possible loss of information about my operation or activity warrant taking steps to reduce or (hopefully) negate the adversary's potential efforts to thwart my operation or activity?" The costs associated with fixing the vulnerability are weighed against the cost of the loss of the data, keeping in mind the likelihood of our data being lost as well as the impact such loss would entail. The managing of Information Protection (IP) requires that a methodological analysis, like the above, should be always carried out on the process/system by information proprietary. Doing that, the information subjective analysis will be reduced and real key protection points will be presented.

III - INFORMATION PROTECTION IN SAFEGUARDS

To apply effective and efficient nuclear safeguards the organization in charge to apply the safeguards should have access to a variety of information and data about the material, process and installation to be safeguarded. On the other hands, the owner of an installation process or technology, either a State or a Company, shall give to the organization in charge to do

the verification some kind of information. This is a basic understanding in any Safeguards Agreement.

In the way of providing the **necessary information and access**, it is built the confidence between the parts and another subjective property, known as transparency, is evaluated by the Safeguards Organization (SO). The dilemma between information protection, which in some cases turns out to be information denial, and transparency, which is an important objective in safeguards, is always present in nuclear safeguards.

The Model Additional Protocol requires much more information and is based on qualitative measures. Besides, the credible assurance and its maintenance on the absence of undeclared materials and activities in a State is likely to require safeguards analysis techniques that more and more will rely on process information access. As long as the Additional Protocol entry into force, the information, and its protection, will have more and more importance.

In order to keep a balance between Openness and Protection, the information to be provided for nuclear safeguards should be submitted to the analysis methodology listed above to determine which information need to be protected. This will be a straightforward and technical evaluation.

Since nuclear safeguards are a matter that usually relates states, politics and non-proliferation some subjective criteria may arise. These additional factors should be considered when dealing with nuclear information that needs to be protected. This will consist of an extra analysis on the information to be provided to the SOs. Among the additional factors we can list:

- The understanding of what it is the necessary information and access. This is always a controversy item between the parties, because the Operator knowing better the technology and its plant capability can infer over certain diversion scenarios much more based on less information. On the other side, the Inspectorate (SO) in its safeguards scenarios analysis sometimes going to paths, truthful or not, which requires additional information that was considered unnecessary by the Operator;
- The release of a non public information or technology. Many States (Operators) complains that they should not give an information on technology that was worldwide denied to them when they tried to get it and was obtained by their own effort and cost. That means - they claim to have the right to deny this technology even knowing that is already on public domain;
- The fear to be halted in the development. Technology holders, when are not yet auto-sufficient, fear that the information provided may show their weakness points and this may be used to halt their progress.
- The trustfulness of the Safeguards Organization. The concern of the States (Operators) if inside the SO the information released will receive the adequate protection and secure;
- The jurisprudence on an information release or allowed access. The state/operator fear that a specific information release or access applied in one safeguards measure turn out to be required by SO as a jurisprudence action.

There are many ways to classify sensitive information data, but relating to nuclear safeguards the most common is to categorize installations and information as Technical sensitive or Commercial sensitive. Technical sensitive are more related to proliferation control and commercial sensitive with business enterprise.

Principles to be used to protect the safeguards information. Tools.

There are many principles, tools and methodologies to use during the information protection. The intention of this paper is not to go in details on this matter, however we would like to comment two basic principles that usually fulfill any information analysis is nuclear safeguards or sensitive technology. These principles should be applied for both, States/Operators representatives and Safeguards Organization agents when dealing with classified information.

The first is the concept of **Need-to-know.**

It is based on the assumption that the owner of the information is expected to ensure that anyone to whom he gives protected information has a legitimate need to know that information. This principle is simple but difficult to implement. In some cases you may need to ask the other person for sufficient information to enable you to make an informed decision about their need-to-know. Need-to-know is difficult to implement as it conflicts with our natural desire to be friendly and helpful. It also requires a level of personal responsibility that many of us find difficult to accept. The importance of limiting sensitive information to those who have a need to know is underscored, however, every time a trusted insider is found to have betrayed that trust.

Difficult situations sometimes arise when talking with friends who used to work with the same protected information that you are now working with. The friend does not have a "need" to keep up to date on sensitive developments after moving to a different assignment. Need-to-know persons are expected to refrain from discussing protected information in hallways, cafeterias, elevators, rest rooms or smoking areas where the discussion may be overheard by persons who do not have a need-to-know the subject of conversation.

Many aspects collaborate to a good need-to-know philosophy application, such as cultural background, defined information managing procedures and procedures enforcement by the organization. The need-to-know philosophy is conflicting with the people friendship and contact, in other words, considering safeguards field, as much as we have the presence of the inspectors in the plant more weak will be the need-to-know enforcement.

The second is the **information containment.**

This principle is based on the assumption that if one have to disclosure some sensitive information from your business or technology one must guarantee that the information will be kept contained as much as possible to the system or persons to which the information is granted. This will require tough procedures on the system or persons with the information. These procedures will be very dependent on:

- the trustfulness of the system or persons that had access to the information
- the systemic environment in which these system or persons manage the accessed information,
- the tools that one have to verify the system or persons that had access to the information
- the effective action that the information proprietary has on these system or persons,

On safeguards, even though the information containment has to be implemented by the information Owner and the SO, it is difficult for the information owner to have an effective control on the containment when the information is released.

IV - SENSITIVE TECHNOLOGIES IN THE NUCLEAR AREA

In the nuclear field, the areas where sensitive information is usually protected to avoid proliferation are:

- Enrichment of fissile material;
- Reprocessing irradiated nuclear fuel to recover produced plutonium;
- Production of heavy water for moderator material; and,
- Plutonium and tritium handling.

Among the proliferation-sensitive nuclear technologies the most important are enrichment and reprocessing, which require relatively complex safeguards approaches to provide assurances that they are not being misused. As these technologies become more widely available, due to the spread of the technology among the countries, the safeguards systems must respond with effective measures for timely detection and verification of declared and undeclared installations fulfilling the information protection requirements.

The enrichment process is much more sensitive when technological information is considered. Even though the theoretical information is available, the development of the enrichment technology (design, special materials, manufacturing, etc.) is still difficult to obtain and requires from the operator/state a certain degree of technological development to

successfully domain the process. Besides, some enrichment processes are very flexible and not requiring huge installations. One the major concern in safeguards is the challenge to detect facilities employing knowing and new enrichment technologies, some of which have small physical footprints and few signatures.

IV - SAFEGUARDS INFORMATION IN CETRIFUGE ENRICHMENT FACILITIES

In the early 1970s, when some states or multi-state organization decide to build enrichment facilities with centrifuges (the gaseous diffusion was already built at that time in Nuclear Weapons States), it seemed that safeguards in that plant would be solved in a relative simple manner by nuclear material accountancy and its verification. The verification looked also a simple task since the uranium hexafluoride (composite in those processes) is kept in closed tube systems and process units, and the verification measures would be performed in some key measurement points.

Nevertheless, the sensitive of the centrifuge technology makes the simple approach questionable when restriction to presence of the inspectors to the cascade hall was arisen in such way to protect the information. At that time the operators of the plant feared for the protection of their know-how and IAEA was concern about its safeguards capacity (to be effective and at same time protect the information obtained). The situation becomes even more complex when certain access points were given to EURATON inspectors and restricted to IAEA inspectors.

At the beginning of 1980s it was establish the Hexapartite Safeguards Project (HSP), composed by Urenco (Germany, The Netherlands and Great Britain), Japan, Australia, United States, the IAEA and EURATOM, which objective is to develop a safeguards approach for centrifuge plants taking in consideration the sensitive information. During the course of the project one line investigated the possibility to have an approach based on “inspection-free” safeguards for the cascade hall (relying on surveillance/containment and other equipment) and the other line including access to the cascade hall.

The first line was abandoned, due to limited measure equipment technology and surveillance at that time. For the second line, where many models with different access rights were considered, and taking in consideration various criteria, including the technology holders concerns on information protection, a solution based on Limited Frequency Unannounced Access (LFUA) was proposed. The LFUA inspections were to be applied under certain conditions, considering among others the time (for access and for the inspection inside the cascade hall), the scope of the verification activities (path to be follow by inspectors, number of inspectors, etc), the type of activities (visual observation, etc.) and the nationality of the inspectors (from a technology holder country).

The main feature of the LFUA model related to the information protection was that the project has reached to a balance between the secrecy problems resulting from inspectors’ access to sensitive information and the fulfillment of IAEA conclusions on the undeclared activities inside the cascade hall through the cascade re-configuration, the presence of non specified equipment and the general features of the facility. It also avoided or turned not necessary the inspector permanent presence at the plant which is considered dangerous for information protection.

Of political significance, the HSP project recognizes that sensitive technology on enrichment shall have a special treatment for guarantee the information protection.

Sensitive Information in Centrifuge Enrichment Facilities.

As we have pointed out earlier the sensitivity of nuclear installation is considered to be technical or commercial. For centrifuge plants the importance of technical details are the most important.

Considering the technical know-how that should be protected, we can divide the centrifuge enrichment process in two parts: the basic element of the process, the centrifuge itself, and the elements working together, the cascade.

- **The centrifuge**: The centrifuge design, manufacturing and assembly are still one of the finest multi-engineering projects in the world. Engineering areas such as mechanical, electrical, materials, electronic, metallurgic and chemical are well combined in this piece of equipment. The most sensitive parts are the centrifuge internals which are very difficult to be seen during a regular announced or unannounced inspection to cascade hall, because de assembly and disassembly must be done with special tools and the nuclear contamination care, and it is performed in special rooms or workshops.
However, the centrifuge externals may still reveal some details of the stage of technology development and in particular may give some clues on how solutions were adopted to surpass some technical breakthroughs when analyzed by experts. External diameter, which has a narrow range of variation due technological limitations, and height, which will be easily estimated on any visual access, are variables for SWU/machine inference but they not carry that importance in sensitive information.
Some operators still have some concerns in full visual access to centrifuges. In this particular, the visual access during inspections for fulfillment of safeguards approach (Production of undeclared and diversion of declared material) must be allowed taking into account the **necessary information and access** concept. The external view of centrifuge itself has a very little hole in the commercial sensitive information.

- **The cascade**: It is in centrifuge cascade that the enrichment process takes volume. The process data, as pressure, flow and other variables are considered very sensitive and also can provided information on the technology stage. It is not uncommon to see the technology holders denying this data when safeguards instrumentation are to be installed in the cascade line. The external view of the cascade shows the instrumentation and connections used which gives the flexibility of the cascade to be reconfigured. Visual access to the cascade lines is important to guarantee that the cascade has not been modified and reconfigured and does not have much restriction on information protection.
The information to be provided through process data and visual access for fulfillment of safeguards approach (Production of HEU material) must be allowed taking into account the **necessary information and access** concept.
The cascade capacities in SWU, nominal and operational have an important hole in the commercial sensitive information. One the safeguards goals is to verify if the plants have the installed SWU declared and if the operation is following the operational SWU declared. That means to detect if any undeclared or not used SWU is being used for diversion. This is evaluated for all the cascades in the plant. Knowing the installation exact SWU that is being used and additional SWU available are very important information on the nuclear enrichment spot and long term market. So, this information shall have to be managed with adequate classification.

- The measures previewed for verification on Safeguards Additional Protocol (articles 2, 4 and 7) will have a great impact on the information disclosure on centrifuge installations. Even though we can apply the called managed access, the verifications on places where the internal parts of the centrifuge can be revealed, such as assembly rooms, decontamination rooms, dismantling rooms and manufacturing facilities on the site certainly should have a strong procedure on information protection.

Protecting the sensitive Information and providing the necessary information and access when applying safeguards in Centrifuge Enrichment Facilities.

When a State/Operator confronts the required information or access by the Safeguards Organization and all considered sensitive points above, the first reaction is to deny the information/access or to create external barrier (physical or human) to protect the sensitive information. What usually happens, the Safeguards Organization will create new measures and/or increase the current measures in order to fulfill its obligation. This process may go on and is not unusual to end up in a set o measures not always sound. Besides, the tendency of these extra measures is to increase the human presence, through the number of inspection or the number of inspectors by inspection.

The best procedure for the State/Operator is to try to make a systematic analysis of the information required by the Safeguards Organization. This analysis should consist on the following:

- The Information or access required must be submitted to the factors analysis listed above for classified information. A classification table is formalized;
- The Information or access required is analyzed considering if it is really necessary for the Safeguards Organization. The principle of Need-to-know is fully used in this analysis. Only the **necessary information and access** should be considered for releasing or allowing. Unnecessary items shall be negotiated with SO;
- The **necessary information and access** required should be submitted to the some additional factors considered by the country (see above). If a negative constraint is applied, by these factors, in any necessary item a new solution should be search to allow the SO to apply the safeguards;
- Among the **necessary information and access** to be released or allowed which ones the State/Operator may substitute for a less sensitive set of measures (information and access). The concept of minimum inspector human presence in the plant should be fully used.

Among the new safeguards tools that we can use to substitute the access to more sensitive information and reduce the inspection effort we can relate:

- Fully use Environmental Sampling technique instead of direct measures techniques that depend upon process data (necessary to open process variable values) for detecting HEU;
- Use of Operator's Measurement System to interchange data with SO. This is the case of allowing the inspectorate to have access in real time to the operator MS and balances/Load Cell indicators. This measure will give the SO the historical information on the process data, not sensitive and will be obtained by other means, and the transparency will reduce the verification measures during inspections;
- Use of more Containment and Surveillance at non-sensitive points. Points where the operator have access to nuclear material, such as product and tails points and sampling points. This will also reduce the inspection effort and human presence at the plant;
- Where is possible to allow remote monitoring or at least the state of health remote monitoring. This will give a better reaction time to the SO also reducing the inspection effort;
- Use of indirect techniques such as mail-box, physical or electronic, to provide data and a real time picture how the plant is operating. The check of this information is simple and gives a better degree of transparency on the SO evaluation. In general, the data furnished will be available in long term period. With the anticipated information provided and its check, by Unannounced inspection or any other means will reduce the measures that otherwise the SO will have to use to verify the plant operation.
- Use of a comprehensive Design Information Verification. The application of some traditional safeguards tools or inspection may be replaced by DIV verification which gives the SO the exact capacity and operational stage of an installation.

The application of these new safeguards tools will give the SO more confidence on the Operator's installation evaluation and will increase the deterrence over any diversion path. Since none of then are based upon large inspection effort that will help also the Operator.

In order to keep a balance between Openness and Protection, the information to be provided for nuclear safeguards should be submitted to the analysis methodology listed above to determine which information need to be protected. This will be a straightforward and technical evaluation. Finally, on the **necessary information and access** to be provided the requirements and procedures for information containment shall be applied.

V – RECOMMENDATIONS AND FINAL REMARKS

Information Protection has an important hole in nuclear safeguards application. When the State/Operator is in the process to provide information or access required by the SO a systematic analysis should be performed based on the points above described. Subjective interpretation of confidentiality must be avoided.

In the nuclear field the concept of **necessary information and access** is one the best tool to avoid proliferation. The non-proliferation measure, through the information protection is responsibility of Operators and also the SO.

Human presence in installation is a great factor for information spreading. Both Operator and SO should consider that when design the safeguards approach for a plant. In centrifuge enrichment plants, due its sensitivity and the necessity of visual observation, the human presence requires special attention.

Over the past few years there have been significant developments in equipment and techniques, suitable for effective enrichment verification activities. These developments can be used without disclosing additional information and helping to reduce the inspection effort, allowing less human presence in the plants and increasing the transparency.

Since the Additional Protocol have to be based on non deterministic measures and on qualitative safeguards tools (verification and analysis) it is certain that more human access will be necessary for covering new activities in the protocol scope (complimentary access). However, the new technological measures mentioned should substitute many traditional activities reducing the inspection impact and leaving for the new activities the challenge to deal with more human presence.

REFERENCES:

[1] Requirements for the protection of safeguards information. NRC Regulations (10 CFR), U.S. Nuclear Regulatory Commission. Washington D.C. February 2004.

[2] Hexapartite Safeguards Project –HSP, Belgium. March 1983.

[3] Wolfgang Fischer and Gotthard Stein, "On-Site Inspections: Experiences from nuclear Safeguarding", Disarmament Forum, 1999.

[4] A. Makhijani, L. Chalmers and B. Smith, "Uranium Enrichment – Just Plain Facts to Fuel an Informed Debate on Nuclear Proliferation and nuclear Power". Institute for Energy and Environmental Research, October 2004.

[5] INFCIRC 254/REV6/Part1, Information Circular on Guidelines for Export of Nuclear Material, Equipment and Technology, IAEA, Vienna, May 2003.