The Environment Council

BNFL NATIONAL STAKEHOLDER DIALOGUE

Security Working Group

December 2004

FINAL REPORT

212 High Holborn
London WC1V 7BF
tel 020 7836 2626
fax 020 7242 1180
email info@envcouncil.org.uk
www.the-environment-council.org.uk

Registered Charity Number 294075 Certificate of Incorporation Number 2004003 VAT Number 577 8121 11

Produced by The Environment Council

December 2004

If you have any comments or queries regarding this report please contact:

Rhuari Bennett
Direct Line: +44 (0) 20 7632 0134
E-mail: rhuarib@envcouncil.org.uk

The process was designed and facilitated by independent facilitator Rowena Harris of BJ Associates for The Environment Council and by Helen Ashley, Maeve O'Keeffe and Rachael Mills of The Environment Council.

212 High Holborn
London WC1V 7BF
tel 020 7836 2626
fax 020 7242 1180
email info@envcouncil.org.uk
www.the-environment-council.org.uk

Registered Charity Number 294075 Certificate of Incorporation Number 2004003 VAT Number 577 8121 11

BNFL NATIONAL STAKEHOLDER DIALOGUE

Security Working Group

Final Report: Executive Summary

Introduction

This report arises from a work stream which formed part of the BNFL National Stakeholder Dialogue. The aim of the Dialogue was *to inform BNFL's decision-making process about the improvement of their environmental performance in the context of their overall development.* The work stream arose from concerns expressed at meetings of the main body of stakeholders to review matters of safety, security and safeguards in the conduct by BNFL of its activities. These concerns led to a proposal to carry out this work stream and to this end to the formation of the Security Working Group (SWG or, the Group).

The Group's purpose and hope was to contribute to the improvement of the security of BNFL's plant and activities, including in particular the transport of nuclear material, by the production of a quality review, using stakeholder dialogue, unique in this security context. The report is the fruit of rare collaborative effort on the part of a number of individuals from a variety of backgrounds with many differences in outlook. Notwithstanding that such differences in view were so divergent that in some instances they appeared to fully contradict each other, the group has produced what it considers to be a constructive and forward looking contribution to the manner in which security is provided for BNFL's activities. This report is now accepted and fully endorsed by the full body of the BNFL National Stakeholder Dialogue.

Methodology

The essential methodology of the study in the report was a journey of several stages. The first part involved the identification of the attributes of an ideal security system for any generic hazardous operation. These attributes were then applied to a nuclear operation and form the standard against which the current situation in BNFL and the UK nuclear security regulatory provisions were examined. The information for this comparison, called the 'gap analysis', was provided in the main from the Director of Security of BNFL and the government's Office for Civil Nuclear Security (OCNS). Where it appeared that a gap existed between the ideal system and the actual position the gap was noted, studied by the group as a whole and a recommendation was made. It is recognised that this gap analysis is open to further review and future studies will lead to further refinement of applied security systems appropriate to the given circumstances.

Recommendations

The outcome of the process, involving nine 2-day meetings between September 2003 and November 2004, is a series of 60 recommendations. These are

addressed to the main parties having responsibilities for the nuclear industry in the United Kingdom, the parties being BNFL, the OCNS, the Nuclear Decommissioning Authority (NDA), and the British Government. The recommendations have been formulated so as to be practical and when implemented will enhance the current practice of security in the UK nuclear industry. It was of considerable benefit to the work of the group that senior members of two main implementing parties, BNFL and the OCNS were represented in the membership of the Group.

To select a number of the recommendations and present them in a synoptic format runs the risk of relegating those recommendations not mentioned to a place of less importance. It is advised that the recommendations be read in full. Therefore, the group decided not to prioritise the recommendations; to do so may form part of future work. The recommendations have however been grouped in seven main categories as follows:-

(a) Funding and resourcing security activities;

(b) Accountability and openness and transparency of information;

(c) Establishing a mechanism for stakeholder dialogue with regard to security issues;

(d) Governance and organisational arrangements with respect to OCNS;

(e) Mechanism for assessing threats (Design Basis Threat), the testing of security measures prescribed by an assessment and forecast consequences of such threats if realised;

(f) Development and application of Security Hazard Indicator for assessment of security impact of an activity or evaluate the cost benefit of a proposed security measure;

(g) National arrangements which fall into remit of government.

In arriving at the various recommendations the group approached the task with an attitude of openness, unrestricted as to the areas to be discussed and the range of measures to be recommended. Inevitably, the group had to operate without having unlimited access to the classified information that would have enabled it to conduct a comprehensive review of the existing security arrangements. In particular the evaluation was made without access to current intelligence as to threats from adversaries (Design Basis Threat). The group was nonetheless given limited classified briefings and a site visit was undertaken at the plant at Sellafield and Barrow Harbour. The evaluation was necessarily taken on trust from BNFL's Director of Security and the members of the OCNS together with the inputs to the group from various professionals involved in the security, emergency and public liaison services. The quality of expertise and advice from these briefings were of considerable assistance in the conduct of the gap analysis and formulating the recommendations. In addition, a considerable input to the recommendations came from the group members in general in the application of their particular expertise and the views of each member drawn from individual career areas and life experiences.

The attitude of BNFL in undertaking to implement, or to lobby for implementation of the recommendations where they lay outside their power (except where it disagrees significantly with the measure and in any such event to give reasons for such disagreement), was helpful in creating trust and enabling the process to move forward.

A number of differences on some security issues which were addressed in the course of the study remain unresolved, such as the manner of transportation of nuclear material, the risks arising from the conduct of plutonium swaps and the degree which sensitive information on nuclear materials should be made available to the public.

A recurrent theme in the course of the study was finding a balance between putting information into the public domain and the need to withhold such information so that it could not come in to the hands of those that would abuse such information for harmful purposes. This matter had a specific bearing on the formulation of the report and of the recommendations as earlier mentioned in the exclusion of certain classified information from the study. The group envisages that all of these issues, and other relevant issues not yet identified be taken forward by a future stakeholder group which may include selected citizens who have security clearance to receive classified information or certain approved types of such information.

While recognising the value of a high quality security system, no such system can provide guarantees of absolute security. Reduction in nuclear activities (including transport of radioactive material) generally results in fewer security risks. The conclusions and recommendations in this report represent the views of those who advocate the immediate cessation of BNFL's nuclear activities, other than the care and management of the existing legacy of nuclear materials. It also represents the views of those who manage and support BNFL's nuclear activities. Therefore, despite the divergence of the two broad outlooks on the larger nuclear issue, the group believes that this report represents a positive contribution and that the recommended actions are a positive step in social and environmental protection from security risks. It is sincerely hoped that it can provide a touchstone for reflecting on the security aspects of nuclear activities and plants, as well as other hazardous activities throughout the world, and to lend considered support to the creation of a safer place for all the inhabitants of the Earth, now and in the future.

Security Working Group 11th November 2004

Foreword

Aim of the BNFL National Dialogue
The BNFL National Dialogue involves a wide range of organisations and individuals interested in or concerned about nuclear issues. Its aim *is to inform BNFL's decision-making process about the improvement of their environmental performance in the context of their overall development.*

The Dialogue is open to national organisations and regional groups as well as expert and specialist concerns. If you would like more information, visit www.the-environment-council.org.uk or contact The Environment Council on 020 7632 0118.

Guidance on Interpreting this Draft Report
The principal purpose of Working Group reports is to inform the deliberations of the Main Group of stakeholders in the Dialogue and any related decisions or activities they might undertake.

Participation (by organisations or individuals) in either the overall Dialogue or the Working Groups must not be taken as an indication of support or disagreement with BNFL's activities.

Any quotes from the reports used in talks, articles, consultation papers and/or other documents published on paper or electronically must be put within the context given within the relevant section of the Working Group's report. The Environment Council strongly advise those considering quoting from the reports to forward their proposed text for review to Rhuari Bennett (e-mail: rhuarib@envcouncil.org.uk)

The role of the convenor
The convenor of the Dialogue is The Environment Council, an independent UK charity. The Environment Council is responsible for designing and facilitating each stage in the Dialogue, and provides relevant support, like issuing invitations and booking venues.

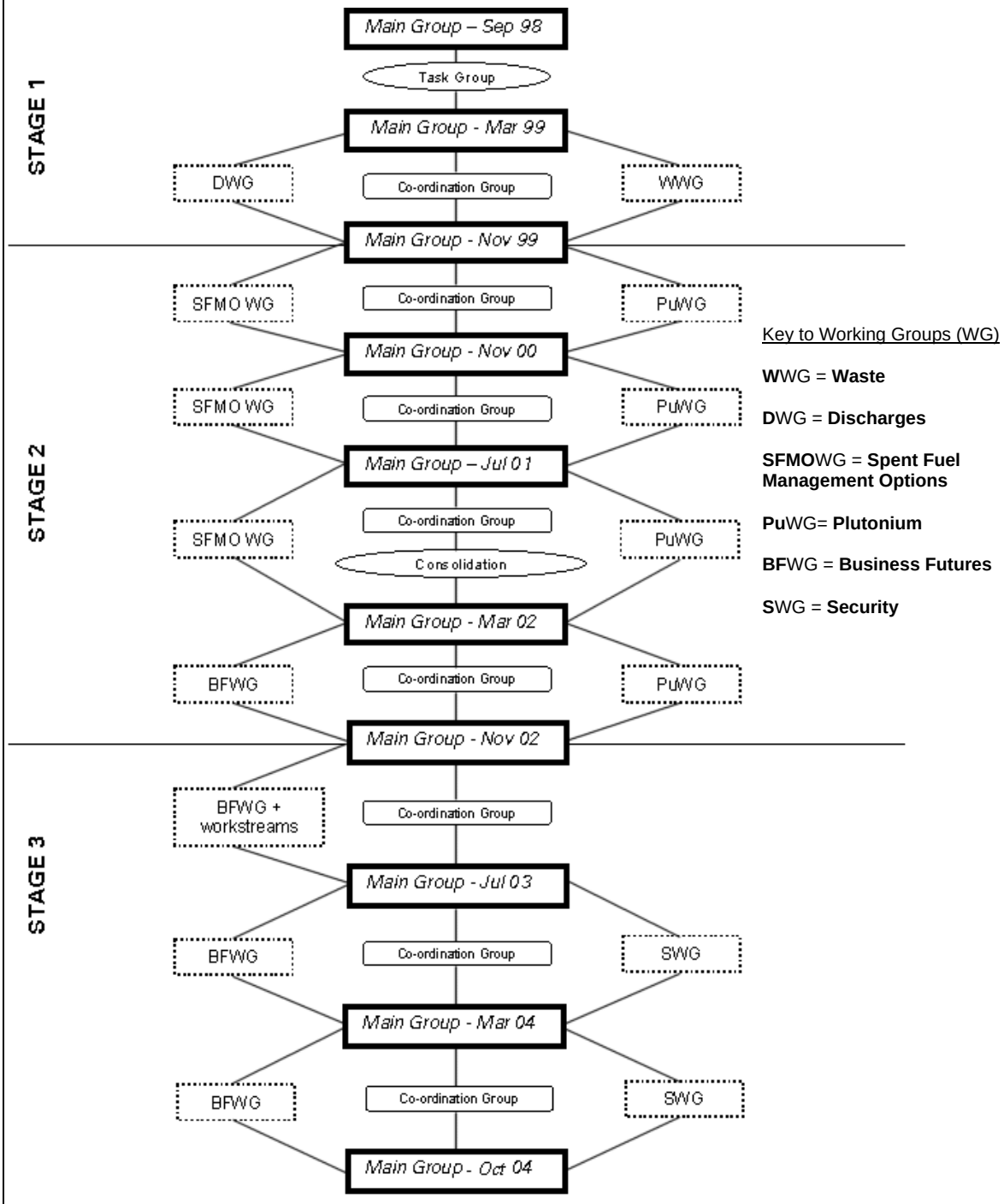
The Environment Council is not responsible for any issue discussed in the Dialogue, and holds no formal position on any of the substantive issues that are or might be considered. It is for the participants to decide what issues are raised, how they might be addressed and how any observations, conclusions and recommendations might be recorded and communicated.

The website of The Environment Council, www.the-environment-council.org.uk displays a full history and evolution of the Dialogue, as well as all of the reports that have been produced from the process.

The Environment Council, December 2004.

History of the BNFL National Stakeholder Dialogue

The diagram below outlines the inception and evolution of the BNFL National Stakeholder Dialogue process. A more detailed history and explanation of each of the groups, together with the reports produced and lists of group members is available at www.the-environment-council.org.uk



Notes:

- The Coordination Group is responsible for providing guidance on linkages and continuity between groups, as well as identifying problems and "potential wobbles".
- "Socio-Economic" and "Transport" issues were discussed throughout the process.

Contact Rhuari Bennett for more information on 0207 632 0134, rhuarib@envcouncil.org.uk

Page intentionally blank

Table of Contents

Appendices

1.0 Introduction

This draft final report of the SWG is provided to the Main Group for approval of findings and endorsement of recommendations. The membership of the Group is given in Annexe 4.

Originally the Group was to examine aspects of safeguards, safety and security. However, due to time constraints and controversy surrounding the interpretation of 'safety', and the implications this would have for the Group in completing its report if it was to deal fully with this issue, the Group agreed to focus exclusively on security issues, with safeguards (proliferation issues) and safety only being examined where these are relevant to the rest of the study.

The Group agreed, in respect of this study, on the definition of 'security' as: "*preventing theft or sabotage*". For the purposes of this work, the focus of study has been on the UK security context.

The key issues identified by the Main Group and endorsed by the initial meetings of this work stream group for examination were:

- International Mixed Oxide Fuel (MOX) trade and transport
- Plutonium Swaps
- UK Transport aspects[1]

Openness and transparency was also identified as a generic factor, and was examined in all the work areas undertaken. These issues were reviewed in the context of the Plutonium Working Group report while taking into account relevant recommendations from other working groups.

International MOX trade and transport: This issue was recognised to be the most important for the Group's consideration. However, there was disagreement over the weighting given to the concerns (security, proliferation and safety), despite widespread discussion.

In view of the proposed MOX shipments by sea within Europe, which have been approved by the Security Regulator, some members of the Group were of the opinion that the different proposed arrangements with regard to these shipments, as compared to MOX shipments to and from Japan, are unacceptable.

It was their judgement that the type of vessel used for these shipments within Europe was primarily dictated by the infrastructure at the destination facilities rather than security considerations. Some members of the Group believe that the vulnerability of the proposed vessel to terrorist attack is substantially higher than the vessels used for the Japanese

[1] Specific relevance to these three work areas are referenced within the matrix in Appendix 1 for each issue considered.

shipments. Therefore application of different security standards to similar nuclear shipments without explanation could cause confusion and concern. Others in the Group believed that current arrangements were appropriate. Once a two-tier stakeholder dialogue process is agreed (see Recommendation 1.8, Section 5.3), the Group recommends that this should be a topic for future stakeholder engagement and that classified information may be assessed.

Plutonium Swaps: This is essentially a safeguards issue. In this instance, the regulator is Euratom (see Operation of Euratom Safeguards in 2002; Report from the Commission to the European Parliament and the Council, 2003). The Group considered whether plutonium swaps would facilitate the diversion of plutonium from its committed end use. The Group also examined whether plutonium swaps would put some plutonium into international commerce earlier than would otherwise be possible (see Annexe 2). The Group was unable to reach a consensus view on this issue.

UK Transport aspects: On UK transport, the Group decided to focus on new areas since the main issues had been extensively explored through dialogue initiatives such as the Cricklewood Dialogue, Jointly Agreed Sampling and Monitoring (JASM), and within Strategic Action Plans (SAP) in the Spent Fuel Management Options Working Group (SFMOWG) and in recommendations from the Plutonium Working Group (PuWG). These aspects have also been studied outside the Dialogue, most recently by the Greater London Authority inquiry. It was suggested, given the time and effort constraints on the proposed group, that transport aspects should focus most usefully on legacy waste management.

The Group recognised that the public's main concern was with the safety issues in respect of the transport of nuclear materials within the UK. There was agreement, however, that the movement of nuclear materials between secured nuclear sites presents additional security concerns.

The Group recognises that the storage, management and transport of nuclear materials presents unique challenges to operators, regulators and stakeholders in respect of information sharing/disclosure.

The Group is cognisant of the need to balance both imparting information which increases public confidence in applicable security systems and providing details which adversaries would find useful. This tension has been central to discussions to date. It is reflected in many of the guiding principles agreed by the Group and statements made in the preamble referring to the need for greater inclusivity of stakeholders in security matters to increase confidence without compromising the integrity of the system.

BNFL representatives in the Group have indicated that BNFL will respond quickly to the final recommendations with the presumption that where BNFL is the accountable body and there is scope to change, change will be implemented. Where proposed and accepted recommendations are outside BNFL's direct accountability, then BNFL will refer and support the recommendations to the responsible agency (e.g. Office for Civil Nuclear Security (OCNS)). Where BNFL cannot support a particular recommendation, the rationale for this decision will be provided. It is understood that BNFL will consider the Group's draft report and recommendations via its Executive Sub-Committee on Security, and that it will

publish its response to those recommendations at the same time as the Group's Final Report is released. The Group welcomes BNFL's commitment to following up the recommendations to this report in a timely manner.

While recognising the value of a high quality security system, no such system can provide guarantees of absolute security. Reduction in nuclear activities (including transport of radioactive material) generally results in fewer security risks. Given that some Group members advocate the cessation of all such activities (legacy management excepted), this report is not to be taken as an endorsement by the Group as a whole of the continuance of nuclear activities.

N.B. The Group found that it had insufficient time to address the whole range of issues relevant to its remit and that on some issues it did discuss (e.g. security on international transport of materials), consensus could not be reached. Nevertheless, where this was the case, the Group has attempted to identify further work that should be carried out to resolve such issues. During the course of the Group's work, discussions unavoidably embraced issues that go wider than those determined by its brief. These relate, in the main, to the nuclear industry's commercial sales of nuclear technology, nuclear plant and material overseas, and the potential impact this may have on future national security and international transport. The Group held a strong cross-section of views on this issue but felt that they fall outside the Terms of Reference (see Annexe 6) and could not be covered within the timescale set for the Group. This report, therefore, does not address such matters.

2.0 Summary of Findings

2.1 Discussion

The Group recognised that the overriding purpose of a security system is the protection of people and prevention of any adverse impacts on the environment, society and the economy (see Preamble, Section 4.1). A secondary consideration is the perception of the level of unnecessary secrecy attached to certain security systems and measures, which some members believed, if addressed, would improve public confidence in security. Other members felt that the focus on public confidence should not have been a primary concern and that the provision of certain security information to the Group to test the robustness of the security system itself should have been central to their work.

The methodology adopted by the Group addressed broader issues of overall concern in relation to security aspects, and their applicability to key issues identified by the Main Group is stated in column 6 of the matrix (Annexe 1). Some members of the Group consistently argued that it would have been preferable to discuss in detail certain key aspects of the security arrangements. However, due to time constraints, the Group's priorities, and present security regulations relating to the release of sensitive information, this discussion did not occur. The Group feels particular consideration needs to be given to how discussions of this degree of sensitivity would be managed in a stakeholder group.

This report cannot capture all the nuances of the detailed discussions both formally in session and between members of the Group outside of session. David Lowry was invited by the Drafting Group to write a discursive paper in an attempt to capture some of this broader discussion. The areas discussed were description of legal arrangements for protection measures, the Design Basis Threat (DBT) and Dirty Bombs. The paper was not discussed in detail by the Group, but the following points have been drawn from the paper. The paper is listed in the index of documents in Annexe 3.

Protection measures are both practical and legal. Other sections of the Group's report discuss various protection measures. The main legal instrument is the 2001 *The Anti-Terrorism, Crime and Security Act*, which has a section on illegal acts in respect of nuclear weapons and weapons materials. Part 8 of the Act is devoted to security of the nuclear industry.

Threat assessments are essential to providing security to the United Kingdom nuclear facilities and materials in transit. The latest annual report from OCNS has a section on threat assessments. Currently for security reasons, the DBT is classified SECRET and no details are published by OCNS. In several meetings the Group found it was unable to have detailed discussions on the adequacy of the counter-terrorism measures unless details of the DBT were made available. The secrecy classification stamped on the DBT was challenged by some Group members. The Group was made aware that the NRC (US Nuclear Regulatory Commission), after extensive deliberation and interaction with the industry and stakeholders, approved changes to the DBT and has published a non-classified summary. No unclassified version of the British DBT has been published or placed before MPs by anyone in a position of authority to know. To the Group'sknowledge no analysis independent of the nuclear security regulator has been conducted of the UK

DBT, because the details of the DBT remain confidential. The Group felt it would be instructive for future stakeholder work to look at how details of the DBT are de-classified elsewhere.

On 18th August 2004, as the text for this report was being prepared, 8 alleged terrorists were charged with conspiracy to commit a "public nuisance" by using radio-active material, toxic gas, chemicals or explosives. This was the first UK court case to inform prosecution for threatened use of a "dirty" radiological bomb, a device to spread radioactive contamination. The issue of the dirty bomb is relevant to nuclear security because radioactive material for a dirty bomb could be stolen from a nuclear site or from nuclear transports.

Fears of a major terrorist attack in the UK, including worries about the possible detonation of a dirty bomb in a major urban area, have grown since 9/11, compounded by the instability created by the invasion of Iraq. Ministers have released plans for the emergency actions that may be needed in the aftermath of a terrorist attack. But concerns remain that insufficient attention has been devoted to radiological remediation. As yet there is no publicly available guidance on the radiological remediation of land and property post-detonation of a dirty bomb.

A number of the recommendations involve several stakeholders taking joint action. This summary captures the key recommendations under the proposed lead stakeholder for that particular aspect, recognising that BNFL in many cases can only lobby for such changes if they agree. A full list of recommendations can be found in Section 5.

2.2 NDA Lead

Whilst the Nuclear Decommissioning Authority (NDA) has made explicit the importance of security in its mission statement, it is unclear at this stage how the NDA perceives 'nuclear security' in terms of its priorities. Funding in relation to security measures required for its Decommissioning and Waste Management programmes need to be made visible to the Treasury. Funding will need to cover regulatory stipulations and OCNS will need to identify its priorities. Additionally, BNFL, as the current operator, will need to highlight current and foreseen security costs. New NDA Decommissioning and Waste Management programmes will necessitate additional demands on security and one area highlighted was the increase in the vetting of personnel associated with more movement of nuclear material within the UK. Such impacts support the development and application of a Security Hazard Indicator and it is recommended that this be used across the overall Decommissioning and Waste Management programme.

Building public confidence in 'nuclear security' necessitates an ongoing dialogue with wide stakeholder participation. The use of reformed Local Liaison Committees (LLCs) or their successors in addressing this issue is supported and recommended, but must be complemented by dialogue at a national level. To be effective, it is essential that such dialogue be properly resourced, including maintenance of the link between the stakeholders and their constituents. As with all dialogues, to maintain the quality of purpose, it should be subject to an ongoing review

2.3 OCNS Lead

To increase public confidence in the Regulator (OCNS), there is a need to demonstrate independence from potential conflicting political and economic pressures. The governance arrangements for OCNS should be reviewed against recommendations made by the Better Regulation Task Force (2003) and in line with Cabinet Office guidelines on Best Practice. The analogy with the Nuclear Installations Inspectorate (NII), which is independent by Statute, is clear and the establishment of a similar authoritative oversight body as the Health and Safety Commission (HSC) should be considered for security issues.

The need for the Regulator to strike a visible balance between the competing need for security and transparency appears throughout the report. The default category is still too often seen as “it cannot be disclosed for security reasons”. A number of recommendations suggest initially taking a more liberal attitude towards disclosure, especially in the case of publishing guidelines or criteria used in the security considerations, or alternatively considering which part could be declassified and generally communicated or shared with a selected audience. Again, the role a reformed LLC or its successor could play within the overall stakeholder engagement process is seen as key and should be explored with the NDA. Having selected the appropriate media in any communication exercise, there is a need to request feedback from the audience regarding the relevance and understanding of the communiqué as part of the ongoing improvement process. Such feedback should be used for all forms of communication and especially for electronic, where the use of a dedicated OCNS web site is proposed as opposed to a shared site. An example of the need for wider communication is the criteria defining particular States of Alert and public broadcasting of the current status.

The DBT featured largely during the Group’s discussions. It forms the core analysis of the perceived threat, and triggers all the precautions taken to counter the threat. Again, as part of the process of building public confidence, the need to convince the public of its robustness and dynamism in responding rapidly to increased threats was seen as key. Recognising that the majority of the content of the DBT cannot be shared, there is perceived to be a benefit from sharing certain aspects more widely. For example, the degree to which systems are tested, including comparison with testing in other countries and the performance outcomes of such tests. Further aspects from within the DBT could be reported to a reformed LLC or their successors, complemented by dialogue at a national level. A presentation on DBT methodology and current threats pertaining should be given to the appropriate Parliamentary Select Committee, probably Trade and Industry.

A wide range of opinions existed within the Group with regard to perceived terrorist threats and consequences, which constantly challenged the claimed robustness of the DBT; and the recommendation for a Joint Fact Finding programme to establish whether it was possible to narrow the range was broadly supported. This could be possibly overseen by reformed LLCs or successor organisations, complemented by dialogue at a national level.

It is recognised that transport operations increase vulnerability and require particular measures to compensate, and that international transport of nuclear material presents particular challenges. Specifically in this regard, it was recommended that OCNS respond

to requests from foreign governments to contribute to briefing programmes within *en route* countries regarding transport of nuclear material.

2.4 BNFL lead

The development of a Security Hazard Indicator is seen as key from the viewpoint of considering the overall security implications of a considered practice as well as assessing the specific benefit that a single additional security measure may provide in relation to its cost. BNFL is currently developing the measure and this work needs to be completed and progressed in conjunction with both OCNS and the NDA. The Group consider it essential that strict corporate oversight of security standards is maintained.

As sponsor of the current National Stakeholder Dialogue and holding the majority of UK experience in relation to the functioning of the current LLCs, BNFL has a major contribution to make to any future stakeholder engagement programme. A number of the recommendations see 'security', and the need for an ongoing dialogue with stakeholders beyond 2005, as a key mechanism in building public confidence and giving reassurance that appropriate measures are being applied to combat world threats.

A number of recommendations refer to clarifying any perceived uncertainties regarding accountability and liability, and to publishing and communicating such information where possible in full, and where not in part. Requesting and monitoring feedback should again form part of any such communication programme and the results should be contrasted against other benchmarks. As mentioned earlier, a broader communication of the current perceived threat being managed is supported but it is recognised that the criteria relating to alert states would need to be better understood by the potential audience initially so as not to cause unnecessary concern through any broader communication.

The perceived range of consequences resulting from a successful terrorist attack varied widely within the Group. A recommendation is made that BNFL initiate a Joint Fact Finding programme (funded by the NDA) to establish whether it is possible to arrive at greater agreement about the range of consequences arising from potential terrorist incidents. The make up of the group is crucial to achieve balance of the cross section of stakeholder views. Emergency response plans are based on the consequences perceived from the worst-case scenario from such incidents. The robust review of such consequences may have implications for the adequacy of the emergency plans and their resourcing.

BNFL is encouraged to use the latest technology to combat the security threat throughout the range of security mechanisms and measures, with value and cost determined by the use of the Security Hazard Indicator.

Demonstration of the security system is seen as key to building public confidence. Recommendations relate to what standards security systems were tested to, the criteria against which they were judged, how they performed, where it is reported and what were the consequences and actions taken. The balance of 'need to know' and 'want to know' is recognised in relation to the sensitivity of some of this information. However, further consideration of what can be and can't be communicated and to what audiences is recommended.

2.5 Government Lead

The Group encourages the Government to do as much as possible to reduce the risk and tension that arises from terrorist threat, recognising that trying to understand the concerns of adversaries forms a fundamental part of any such programme.

The benefits of a stakeholder dialogue appear to be recognised by the Government in terms of the legislation, governance and review bodies it has established to address the issues of nuclear waste management. However, no provision is made within the Energy Act 2004 for funding broader dialogues as recommended within the Group's report. Without adequate funding, no dialogue can be successful.

The Treasury needs to be aware of the ongoing requirements and consequential costs for the provision and regulation of the overall security system associated with the industry. Additional appropriate funding and resources may be required for emergency planning and emergency services post any such incident, and this should be reviewed.

With regard to 'security governance', the Government should respond positively to any proposed new arrangements to achieve a greater degree of independence for the regulator OCNS. Additional consideration should be given by Ministers to formalising Parliamentary oversight of the civil nuclear security arrangements and the annual report published by OCNS. As part of any such overall review, the clear responsibilities and liabilities of both the Regulator and Operator with respect to terrorist activity need to be clarified.

Inconsistencies and omissions identified in current regulations should be resolved. In order to come to an informed view of whether a balance is being struck between the demands of security and the need for transparency with respect to information currently provided by OCNS and BNFL, it is recommended that the Government classification guides relevant to civil nuclear security are published.

3.0 Methodology

The Group initially agreed to identify the attributes of an ideal security system for a facility dealing with hazardous materials. The purpose was to allow generic attributes relevant to any hazardous activity to be identified, enabling a comparison through debate on how these would apply to, and any additional specific attributes that might be necessary in respect of, the nuclear industry.

The ideal attributes were examined from three perspectives:

- The public (including local communities, local authorities and pressure groups) – what are their concerns, what would give confidence and what do they want to know?
- The Government, industry and regulators – what is feasible, and what information can be safely made available?
- Terrorists or adversaries – what do they want to find out to help them mount a successful attack and how might they find this information out?

The ideal attributes were then consolidated (see Section 4 below). The Working Group also felt that the attributes should be placed within a proper context and has prepared an explanatory preamble (also in Section 4).

The substantive part of the Group's work therefore involved the identification of the attributes of an ideal security system as they related to the nuclear industry. The Group then created a matrix that allowed comparison with the existing system, facilitating a gap analysis between the two. Information regarding the existing system was provided to the Group from the two viewpoints of the Security Regulator (OCNS) and BNFL's Security Director. OCNS provided the information regarding the current principles applied within the UK nuclear industry. This included the international framework provided through conventions and International Atomic Energy Agency (IAEA) guidance; the UK government mechanisms and responsible agencies and the applicable legislation and regulations, including DBT analysis in the context of security planning and the relevant enforcement powers application. These views are reflected in the matrix (Annexe 1): column 2 is a purely BNFL view; column 3 is a regulatory view; the analysis is a Group activity.

The Group additionally heard from transport experts from both OCNS and BNFL, the Chief Emergency Planning Officer from Cumbria County Council, BNFL's Public Affairs Department regarding the activities of the Local Liaison Committee (LLC), and representatives from the UK Atomic Energy Agency Constabulary (UKAEAC). The Group also visited the Sellafield site and the Barrow terminal to inspect their security arrangements.

Inevitably, this process gave a predominantly Official, Regulatory/BNFL perspective, which the Group was required to take on trust in terms of its interpretation and robustness. Additional information was provided by several Group members that gave different/ contradictory perspectives (these documents are listed in Annexe 3, although not all have been discussed by the Group). The Group recognises that there exists a much greater

volume of information which it did not have time to review or analyse within the working timeframe, for example the July 2004 Parliamentary Office of Science and Technology (POST) 'Assessing the Risk of Terrorist Attacks on Nuclear Facilities' (Appendix 1).

The gap analysis allowed conclusions and recommendations to be drawn, which can be found in Section 5. The Group recognised that some gaps were created, not by the comparison of two attributes, but by the absence of information relating to a particular issue, and where this occurred it is made clear in the recommendations. The analysis identified deficiencies in the system, but the Group was keen to ensure that the recommendations also included positive steps that could be taken to improve the system. These recommendations will be fed into the overall consolidation process being conducted by the Co-ordination Group of the Dialogue and passed to the appropriate bodies, including the BNFL's Executive Sub-Committee on Security.

In following this methodology, some Group members felt it did not allow enough time to fully discuss some substantive areas of concern, e.g. content of the DBT. Nevertheless, there was agreement to proceed with this methodology on the grounds that it gave the Group the opportunity to discuss the broad range of security issues.

4.0 Attributes of an Ideal Security System

4.1 Preamble

The values and freedoms of any political and social system are necessarily related to the security measures required to protect them. The degree to which these security measures are enforced and the consequent impact on the population on whose behalf the freedoms are being protected has always been an issue. In recent years, this has been brought sharply into focus by the rise of terrorism and the security responses provoked by that rise. The striking of a balance between public protection and the erosion of the very freedoms those safeguards are designed to protect is perhaps the greatest challenge faced by society today. Even with draconian erosion of civil liberties, any society could not afford its people total protection.

In the past, security and the need for secrecy it engenders has often been used – sometimes unreasonably - as an excuse for the non-disclosure of all but the most trivial of information. As the desire for greater transparency increases, this blanket response of ‘security is not discussed’ is no longer appropriate. This must give way to a more considered and proportionate response to requests for information if the principles of openness and transparency within decision-making processes are to be realised. While we examine ways of achieving these goals, we should be keenly aware that there are some threats, particularly the invidious nature of terrorism, against which democracies will always be vulnerable.

The attributes detailed below seek to identify key elements of an ideal security system covering a high hazard industry, together with measures against which its efficiency and robustness could be gauged.

The adversaries against whom these measures are ranged may be anonymous and mysterious to us and every effort must be made to try to understand their motives, demands and objectives if the security regime is to be effective.

Since September 11, 2001, and in the wake of subsequent other major international terrorist events, it has become evermore apparent that diplomatic efforts are central to the reduction of the threat level from terrorism. We must attempt to reduce the threat by understanding and working tirelessly to resolve demands and perceptions of injustice if we are to create an international society in which cultures and peoples are less polarised. Security measures are only an adjunct to diplomacy; they are not a single long-term solution to the problem.

An ideal security system would deliver robust protection based on the attributes below and without employing unnecessary secrecy that restricts democratic openness and undermines public confidence.

4.2 Attributes of an Ideal Security System

1. Overarching Attributes

A robust and optimum security system will:

1.1 Make transparently clear at all levels where responsibilities and accountabilities lie, including those relating to the on-going provision of adequate funding. Such transparency should include a clear indication of what the responsibilities are, how they are discharged, what dispute procedures exist and what monitoring systems are available to ensure enforcement.

1.2 Make transparently clear at all levels how decisions are arrived at, by whom and against what criteria, and how they may be changed or influenced.

1.3 Ensure that a balance is struck between the demands of security and the needs for transparency to prevent either one undermining the other.

1.4 Recognise and explain that there is no risk-free situation and that the need for vigilance is constant.

1.5 Recognise that while we must work to reduce threats to the fullest extent possible, we must also anticipate consequences and act accordingly in order to protect public safety and the environment.

1.6 Demonstrate the justification of the security regime in terms of its purpose, legality, and compliance with regulations and provide a mechanism through which this demonstration could be conducted.

1.7 Ensure that an increase in the sophistication or robustness of a security system can demonstrably reduce the risk and that it's economically justified on the basis of a cost/benefit analysis.

1.8 Deliver effective security on the ground, whilst understanding and responding to stakeholder concerns.

1.9 Ensure that security regulations address the potential misuse and theft of hazardous materials, without impairing their availability for use, and ensure safe management of such materials including their removal and storage after use.

1.10 Minimise risk by careful consideration of siting of plant, building, equipment and transportation operation.

1.11 Demonstrate an appropriate state of alert at all times.

1.12 Be adequately resourced.

1.13 Be subject to testing, demonstration and exercise on a rolling basis in order to prove adequacy, and improve where necessary, and continue to make relevant to the design of security measures.

1.14 Recognise that transport operations increase vulnerability and require particular measures to compensate.

1.15 Be based on the need to counteract the capability and intentions of the adversary, not on the probability of attack.

1.16 Ensure that security measures are integrated into national security and response arrangements.

1.17 Make provision for all possible steps to be taken to deny terrorists and other adversaries the opportunity to obtain funds, financing and materials for their operations.

1.18 Ensure that the arrangements are comprehensive, effective, and address such measures as the security of IT systems, physical security, personnel security, etc.

2. Attributes Relevant to Regulation

A robust and optimum security system will:

2.1 Be transparent, enforceable and capable of generating public confidence.

2.2 Comply with international, state, regional and local statute.

2.3 Generate confidence in the regulatory bodies that they meet their statutory obligations and comprise of demonstrably competent experts and be appropriately resourced.

2.4 Be subject to 'independent' review and scrutiny through a transparent mechanism developed with stakeholder input and approval.

2.5 Be subject to a regulatory system run by regulators who are independent of policy makers, the industry and other vested interests.

2.6 Take account of the growing likelihood of litigation should security be breached.

3. Attributes Relevant to Systems

A robust and optimum security system will:

3.1 Be designed to encourage and enhance public and stakeholder confidence in the owners and operators and in those accountable for security.

3.2 Involve a robust access control system.

3.3 Be designed to combat all levels of capability and intention, and flexible enough to respond to perceived level of threat at any given time.

3.4 Ensure thorough and ongoing vetting of staff, contractors and visitors to avoid infiltration of terrorists and other adversaries, and ensure that systems are sufficiently thorough to give high confidence in the identity, credentials and ongoing trustworthiness of personnel, including vulnerability to corruption.

3.5 Test the capabilities of the system to defeat the simulated adversary and ensure the tests themselves are realistic and unbiased.

3.6 Accommodate the need for continuous and integrated analysis of the threat and intention level. Information resulting from such analysis should be made available to all parties concerned with the security of operations.

3.7 Be subject to a comprehensive performance management system.

3.8 Not rely primarily upon secrecy.

3.9 Above minimum standards, ensure the security in place (including response measure) is not predictable by observation by the adversary.

3.10 Contemplate the ending or suspension of a particular activity if the system fails the tests against the adversary's capabilities.

3.11 Guard against cyber-terrorist threats by making computer systems secure and against unauthorised interference.

3.12 Be capable of monitoring communications and infiltrating terrorist networks to disrupt their modus operandi with the aim of rendering them ineffective.

3.13 Be capable of accommodating an independent peer review assessment of consequences in all potentially hazardous facilities and services.

3.14 Establish security priorities and regimes through a transparent mechanism developed with stakeholder approval and input.

3.15 Ensure that only those with an operational need to access sensitive materials and information can do so, in store, process or transit.

3.16 Be a combination of physical protection, effective safeguards and stock control and provide adequate assurance that nothing has gone missing.

4. Attributes Relevant to Information Provision

A robust and optimum security system will:

4.1 Presume that information should be provided but recognise that there exists a need to strike a balance between public trust and risks associated with what is disclosed or withheld within statutory and administrative limits and requirements.

4.2 Be capable of de-sensitising information (reclassified by reducing sensitivity, e.g. omitting certain material) to make it useable to the public and emergency services.

4.3 Aim at enhancing public confidence in the information disclosure system through the provision of security and emergency response information.

4.4 Agree channels for the provision of information (e.g. websites, texting linked to the national network and publications which clearly explain what the emergency response embraces, sirens, point of contact, escape routes, muster points, what to expect, who to ask questions, anticipated flood of calls and requests in the event of an incident which requires the invoking of the emergency plan).

4.5 Provide all information for the public in a clear and digestible form.

4.6 Communicate that the system is responsive to changing circumstances.

4.7 Put in place structures for rigorous stakeholder consultation. Ensure that body develops and applies criteria relating to what information it is appropriate to withhold.

4.8 Be flexible in its reporting regime and capable of communicating different things to different audiences.

4.9 Maintain healthy and viable links between stakeholder representatives and their constituents.

4.10 Where trans-frontier shipments of hazardous materials are involved, provision should be made to extend the consultation process to acknowledge and accommodate as appropriate the international dimension.

5.0 Recommendations to the Main Group

5.1 Recommendations to the Main Group

The Group welcomes the assurance from BNFL management, in respect of this Group's report, that where 'gaps' are identified and recommendations made they will either:

- Implement changes if they agree with the findings, if they are within BNFL's control and have the funding to do it
- Lobby for changes if they agree with the findings but where implementation of, or funding of, the changes are outside their control
- Explain the reasons why they will not implement the changes if they don't agree with the findings

The Group recognises that in the future several of the responsibilities currently held by BNFL will transfer to the NDA. Therefore, we would strongly encourage those successor organisations, including the NDA, to adopt those recommendations which are relevant to their responsibilities. In particular, the Group strongly recommends that those issues that it has been unable to discuss in adequate detail be pursued as a matter of urgency.

The Group recommends that the Main Group approves the findings and endorses the recommendations. The 60 full recommendations are detailed in the Recommendations and Conclusions Table on page 20.

The Group was able to categorise the recommendations according to the following descriptions in order to highlight the areas that most need attention. The responsibilities for taking action are identified in the Summary of Findings (Section 2 above), which emphasises the key findings from the Group[2]

Recommendation 1: The Group recommends that the Main Group endorse the recommendations related to funding or resourcing activities associated with security (Recommendation Category A)

Recommendation Numbers (see table below)	1.1a	2.6	4.4
	1.5		4.6
	1.9		
	1.12		

[2] The number of recommendations under each heading is not necessarily indicative of the relative significance of each category.

Recommendation 2: The Group recommends that the Main Group endorses the recommendations related to achieving clarity of accountability and openness and transparency of information where possible (Recommendation Category B)

Recommendation Numbers (see table below)

1.1b	2.1	3.4 (2)	4.3 (3)
1.1c	2.4	3.10 (3)	4.8 (3)
1.2a		3.7	4.10
1.2b			
1.3a (3)			
1.3b			
1.10a			
1.11			
1.18			

Recommendation 3: The Group recommends that the Main Group endorses the recommendations related to establishing a mechanism for stakeholder dialogue with regard to security issues (Recommendation Category C)

Recommendation Numbers (see table below)

1.8	4.7	
	4.9 (2)	

Recommendation 4: The Group recommends that the Main Group endorses the recommendations related to the governance and organisational arrangements with respect to OCNS (Recommendation Category D)

Recommendation Numbers (see table below)

1.12	2.3	3.6

Recommendation 5: The Group recommends that the Main Group endorses the recommendations related to the mechanism for assessing threats (DBT), the testing of security measures prescribed by the assessment, and the forecast consequences of such threats if realised (Recommendation Category E)

Recommendation Numbers (see table below)

1.4 (2)	3.3	4.4
1.10c	3.5	
1.11	3.13	
1.13 (2)		
1.14 (2)		

Recommendation 6: The Group recommends that the Main Group endorses the recommendations related to the development and application of a Security Hazard Indicator to both assess the security impact of an activity or evaluate the cost/benefit of a proposed security measure (Recommendation Category F)		
Recommendation Numbers (see table below)	1.7	3.2
	1.10b (2)	3.10

Recommendation 7: The Group recommends that the Main Group endorses the recommendations related to national arrangements which fall within the remit of Government (Recommendation Category G)		
Recommendation Numbers (see table below)	1.4 1.6b	4.8

5.2 BNFL's Response to the SWG recommendations

A commitment made by BNFL at the commencement of the SWG was that it would respond to the recommendations in a timely manner. The draft report was referred to the Executive Sub-Committee on Security (ECS) in October 2004 with a recommendation from the Security Director that the SWG recommendations should be accepted, subject to further consideration in two areas (relating to the definition and communication of Alert States, see recommendation 1.11, and the possible mis-interpretation of recommendation 1.9 relating to uncapped liabilities). The ECS approved the Security Director's recommendation and highlighted two further areas that were of concern:

1. The Committee considered that the SWG recommendations were more applicable to Sellafield than other sites operated by BNFL that have lower security categorisations. Its view was that the recommendations do not necessarily apply equally to all sites.
2. That BNFL should be accepting potentially significant security workstreams and consequential financial implications in the period immediately prior to the transition to NDA of ownership and funding. The Chairman of the ECS reminded the Committee that BNFL had agreed to implement those enhancements that could be funded and to lobby for change if outside BNFL's control.

Specific responses to the 60 recommendations have been incorporated into the table below.

5.3 Recommendations and Conclusions Table

The table below shows the conclusions and recommendations drawn from the gap analysis matrix (see Annexe 1).

The recommendations are allocated to six categories:

A: These Recommendations are related to funding or resourcing activities associated with security.

B: These Recommendations are related to achieving clarity of accountability and openness and transparency of information where possible.

C: These Recommendations relate to establishing a mechanism for stakeholder dialogue with regard to security issues.

D: These Recommendations relate to the governance and organisational arrangements with respect to OCNS

E: These Recommendations relate to the mechanism for assessing threats (DBT), the testing of security measures prescribed by the assessment, and the forecast consequences of such threats if realised.

F: These Recommendations relate to the development and application of a Security Hazard Indicator to both assess the security impact of an activity or evaluate the cost/benefit of a proposed security measure.

G: These Recommendations relate to national arrangements which fall within the remit of Government.

1. Overarching Attributes

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
1.1a	A	There is currently uncertainty about future funding for security measures.	The NDA to make transparently clear to OCNS and interested stakeholders that the funding for effective security arrangements is available.	NDA	This should happen prior to April 2005.	Agreed
1.1b	B	The current iteration of the OCNS Disclosure Guidance declines to publish security standards on security grounds to prevent possible mis-use. Some members of the Group have commented that the proposed restrictions on the information disclosure on radioactive waste are too tight.	The Group believes that there needs to be continuous examination by relevant stakeholders (including consideration of a two-tier stakeholder engagement framework) of the arguments for and against the withholding of specific types of information. At this stage, OCNS should specifically review the reason for non-disclosure of information on radioactive waste.	OCNS	Ongoing	Agreed
1.1c	B	NISR 2003 text does not include dispute procedures – operators/ regulators/NDA.	Make sure Amendment to NISR 2003 includes dispute procedure.	OCNS	Initiated through Government by Dti at the next amendment.	Agreed
1.2a	B	Need to make transparently clear at all levels how decisions are arrived at, by whom and against what criteria, and how they may be changed or influenced.	Finalise MoU between BNFL and UKAEAC to avoid any mis-understanding over accountabilities and decision-making, including the use of force.	BNFL	June 2005	Agreed
1.2b	B	It is unclear to the Group why information on the MoU re accountabilities and decision-making between BNFL and the UKAEAC is classified.	BNFL needs to explore with the UKEAAC and others the possibility of de-classifying all or releasing parts of this document.	BNFL	June 2005	Agreed
1.3a	B	There is insufficient information available from OCNS and	Publish civil nuclear classification guides or explain why they are classified.	OCNS	June 2006	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
1.3a	B	BNFL to establish whether a balance is being struck between the demands of security and the need for transparency.	BNFL should include a couple of questions on nuclear security on existing public and stakeholder opinion polls and develop a baseline to establish whether the release of more information dealing with nuclear security increases public confidence.	BNFL	December 2004	Agreed
1.3a	B		OCNS should monitor and report back to stakeholders the number of visits to its Disclosure Guidance document posted on its website to give an indication of interest.	OCNS	Results by the next OCNS annual report (May/June 2005)	Agreed
1.3b	B	FoI Act is as yet untried in relation to security in the nuclear industry and it is not clear whether the rules on disclosure will be successfully challenged by the public.	BNFL should evaluate the FoI Act to determine the extent to which BNFL can go beyond its provisions for restricting information to the public in order to increase confidence and publish how it complies with the Act.	BNFL	Publication of compliance with and evaluation of FoIA by end January 2005.	Agreed
1.4	E	Unavailability of DBT makes it impossible for external analysis of any gaps.	OCNS should ensure the DBT is dynamic and takes into account as many threat scenarios and consequences as possible.	OCNS	Ongoing	Agreed
1.4	E		OCNS to publish as many aspects of the DBT as possible, as is done in the United States, to demonstrate as robust a response as possible and to increase public confidence.	OCNS	April 2005	Agreed
1.4	G		Government should seek to reduce the level of terrorist threat by vigilance, but also by trying to understand the views and concerns of adversaries.	Government	Ongoing	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
1.5	A	The Group and Professional Emergency Planners recognise that there are chronically inadequate national resources to deal with a major emergency.	Appropriate resources should be put into emergency planning and post-incident response (see 4.4).	Government NDA	Ongoing	Agreed
1.6a	-	Some of the information necessary to provide justification is sensitive and cannot be made available to all.	See 1.4			
1.6b	G	The law at the moment is totally insufficient in relation to intruders. There is a tension between the right to demonstrate and the need to protect against unauthorised intruders who might present a terrorist threat.	Examine the law in relation to trespassing at airports, the Channel Tunnel and nuclear installations in other countries.	Government	As soon as possible. Target date 2005.	Agreed
1.7	F	Any increased costs incurred in the improvement in the security system have to be justified against benefits in terms of reduction of threat.	The development of a Security Hazard Indicator would assist in principle in this task and would enable people to see the cost benefit of spend.	BNFL	December 2004	Agreed
1.8	C	There is no formal mechanism for dialogue with a broad cross-section of stakeholders on nuclear security measures.	BNFL should support, expedite and participate in as appropriate the reform of the existing Local Liaison Committee (LLC) system, in conjunction with the Nuclear Decommissioning Authority (NDA), to establish site-based and transport-related engagement processes, which include a security element drawn from some of the LLC stakeholders who will require additional security vetting. OCNS should have active participation in any new arrangement to ensure that the	BNFL	The stakeholder group is established by April 2005.	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
			broader national and international security aspects are addressed through this stakeholder process.			
1.9	A	It is inappropriate to allow economic concerns to override the need for security.	BNFL should never allow economic concerns to override security needs and be prepared to provide justification when challenged.	BNFL	Ongoing	Agreed
1.10a	B	The siting of buildings on nuclear sites has not, in the past, been determined or significantly influenced by security considerations.	BNFL should have formal procedures in place that make an assessment of security implications a prerequisite in its building siting policy.	BNFL	January 2005	Agreed
1.10b	F	Absence of a national analysis and strategy for making decisions on the inevitable dynamic tension between continued onsite storage and centralised storage, which involves transport.	Make sure that policy on new building siting and changes in existing buildings are subject to Security Hazard Indicator analysis.	BNFL	Ongoing from January 2005	Agreed
1.10b	F		The NDA should inherit and develop the Security Hazard Indicator and apply this to minimise the overall movement of radioactive materials (and hence terrorist risk) which it will be required to manage through its decommissioning programme.	NDA	Ongoing from April 2005	Agreed
1.10c	E	Effective security assumes effective safety measures. Doubts have been raised about the effectiveness of the safety regime when it comes to transport containers. The doubts are based on the current sequential testing system for the resistance of shipping flasks to fire, impact and immersion, which may not simulate the concurrent effects of real life accidents and thus	OCNS needs to ensure that the results of the test programme are properly considered by the appropriate safety and security authorities.	OCNS	April 2006	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
		offer less than anticipated protection against the effects of actual attacks.				
1.11	E	Security must be adequate to defend against attack that comes without warning and not be subject to political manipulation.	OCNS should make the explanation of states of alert publicly available. OCNS should also ensure that states of alert are always based on objective circumstances, should reflect the real situation and not be subject to political manipulation.	OCNS	April 2005	Agreed
1.11	B		BNFL should make it clear to the potentially affected public what the states of alert mean and their implications on emergency response. BNFL should also commit to regular communication of the state of alert at the facility to the local population by appropriate media.	BNFL	From April 2005	Needs further consideration
1.12	A	Treasury should be fully briefed on the importance of the continued funding of security arrangements. As noted in 1.1, the situation post NDA formation needs to be considered. There is no formal procedure for determining OCNS resources.	All appropriate agencies (e.g. NDA, Department for Trade and Industry (Dti), BNFL) should ensure that the importance of this issue is communicated forcefully to the Treasury, including appropriate staffing and resourcing levels within OCNS.	NDA BNFL OCNS	Prior to April 2005	Agreed
1.12	D		The governance arrangements for OCNS should include an annual examination of resource needs. The OCNS budget should be published annually.	Government	June 2005 and annually	Agreed
1.12	-		See 1.1.			
1.13	E	The way in which exercises are currently carried out relies on the UKAEAC to play too many	BNFL should review with OCNS whether completely independent personnel should be used as the simulated adversary.	BNFL OCNS	From April 2005	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
1.13	E	roles. For example, they would take the role of exercise commander, adversary and defence force. There are only so many things you can simulate using people, for example it is not feasible to simulate mortar attacks except on military ranges.	Advanced computer simulations should be used to enhance the realism and range of scenarios that can be tested.	BNFL	From April 2006	Agreed
1.14a	E	Security plans should always put the priority on countering potential threat, not on minimizing the potential costs.	see 1.9			
1.14b	E	The application of different security standards to similar nuclear shipments without explanation causes confusion and concern.	This could be a topic for future stakeholder engagement. Classified information may be assessed in a two-tier stakeholder dialogue process (see 1.8).	Stakeholders BNFL OCNS	After April 2005	Agreed
1.15	-	Possible infiltration of legitimate protest group not addressed.	See 1.4 and 1.7			Agreed
1.16	NO IDENTIFIED GAP					
1.17	NO IDENTIFIED GAP					
1.18	B	The Regulations governing the security of non-nuclear but radioactive hazards (such as sealed sources) are not as comprehensive, e.g. vetting of drivers.	OCNS should bring inconsistencies in regulations covering radioactive substances to the attention of policy makers in Government so that regulations are consistent, because it has a direct bearing on the public perception of nuclear security.	OCNS	Current	Agreed

2. Attributes Relevant to Regulation

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
2.1	B	The level of public confidence in the security regulations is not known.	BNFL and OCNS should take all necessary measures to increase and monitor public confidence in their security systems including a) monitoring responses to all information put into the public domain and b) appending questions to documentation requesting feedback on user friendliness, etc.	BNFL OCNS	 Publication of OCNS annual report (May/June 2005)	Agreed
2.2	NO IDENTIFIED GAP					
2.3	D	The Cabinet Office guidelines on best practice need to be examined.	OCNS should be established along similar lines to the NII to achieve a degree of independence from potential Government pressure. Cabinet Office guidelines on best practice should be adopted in this process.	OCNS	By April 2005	Agreed
2.4	B	Governance arrangements and mechanisms for independent review of OCNS are currently too narrowly drawn.	OCNS should make representations to Government to extend the membership of its advisory board to include suitably a qualified representative from a broader base of stakeholders, including Non-Government Organisations (NGOs), in order to provide a range of perspectives to allow for balanced discussion.	OCNS	April 2005	Agreed
2.5	-	See 2.3 and 2.4				
2.6	A	It's unclear where, if at all, BNFL's and OCNS's corporate liability currently lies with respect to terrorist incidents	BNFL and OCNS independently should confirm whether, under current legal arrangements and guidance notes, they have clearly identifiable responsibilities and appropriate funds for compensation, in respect of the consequences of terrorist incidents. If not, the situation should be rectified.	BNFL OCNS	July 2005	Agreed

3. Attributes Relevant to Systems

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
3.1	-	See 1.3, 2.3 and 4.9				
3.2	F	There's always a risk associated with identity management. The debate on this issue is in the public domain.	BNFL should be aware of the latest technology being applied in this area, but should also take into account cost benefits through the Security Hazard Indicator.	BNFL	Ongoing	Agreed
3.3	-	There is a gap between all possible levels of capability including the most unlikely and those threats which are encompassed within the DBT (see Preamble – Section 4.1 of Report).	See 1.4			
3.3	E		As part of its programme of increasing public confidence and understanding of the DBT methodology and the judgments made, OCNS should consider a presentation to the relevant Parliamentary Select Committee (Trade & Industry).	OCNS	July 2005	Agreed
3.4	B	With the advent of the NDA and the potential for a much greater degree of contractorisation, additional vulnerabilities in vetting may arise. Potential increases in nuclear transport movements linked to decommissioning may result in the need to have a significantly higher number of personnel, particularly drivers, vetted.	Sufficient information should be provided by OCNS (the vetting agency), following consultation with the vettee, to BNFL to manage any potential risk.	OCNS	April 2005	Agreed
3.4	B		As a minimum, vetting agencies should consider making the criteria used for vetting available to BNFL.	OCNS	April 2005	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
3.5	E	There's a limitation to what you can realistically exercise on operational sites or on transport. The adversaries are usually played by UKAEAC officers and there could be a tendency for them to employ predictable methods and techniques.	BNFL and OCNS should keep under review all system testing used by other security agencies, including force-on-force exercises.	BNFL OCNS	Initiate by April 2005	Agreed
3.5	-		See 1.13			
3.6	D	No visible or convincing mechanism for holding OCNS to account for its performance, including the dissemination of relevant intelligence.	The OCNS should consider a management statement as recommended by the Better Regulation Task Force (2003) which could potentially be met by the establishment of an authoritative and independent oversight body. See 2.3 and 2.4.	OCNS	April 2005	Agreed
3.7	B	See 4.3 Retain strict corporate oversight of security within BNFL.	BNFL should retain its corporate Security Directorate to ensure corporate oversight of security standards is maintained.	BNFL	Ongoing	Agreed
3.8	NO IDENTIFIED GAP					
3.9	NO IDENTIFIED GAP					
3.10	B	It is currently not possible for stakeholders to assess whether security arrangements in place have failed a test against an adversary's capabilities.	The results of security exercises should be included in BNFL's formal security assessment systems. Vulnerability assessment should be at the level of individual facilities rather than at a more generic site level.	BNFL	December 2004	Needs further consideration
3.10	B		In order to facilitate stakeholder assessment of the robustness of the system, BNFL should consider making the above available to LLCs or their successors, complemented by dialogue at a national level.	BNFL	From April 2005	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
3.10	F		The development of a Security Hazard Indicator should be completed as a matter of urgency and it's results used to prioritise the decommissioning of potentially hazardous facilities.	BNFL	December 2004	Agreed
3.10	B		BNFL and OCNS should determine and publish the criteria used to judge whether the security system has failed to the extent that leads to the consequence of that operation ceasing.	OCNS BNFL	In OCNS annual report	Agreed
3.11	NO IDENTIFIED GAP					
3.12	OUTSIDE OF GROUP'S REMIT					
3.13	E	There are seriously divergent views regarding consequences of terrorist incidents considering hazardous facilities and services. The Group is uncertain as to whether these can ever be reconciled.	BNFL should initiate a Joint Fact Finding programme with LLCs or their successors (funded by the NDA), complemented by dialogue at a national level, to establish whether it is possible to arrive at greater agreement about the range of consequences arising from potential terrorist acts as defined in the DBT. The Group recognises that this is conditional upon the establishment of a two-tier stakeholder engagement process.	BNFL NDA	After April 2005	Agreed
3.14	-	There is opaqueness at the moment because the only stakeholders involved are the industry and policy officials.	See 1.8 and 4.7			
3.15	-	There is ultimately an irreconcilable gap between 'need to know' and 'want to know'. The Group's proposal for extending the remit of the LLC could go some way in narrowing this gap.	See 1.8 and 4.7			

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
3.16	-	NO IDENTIFIED GAP Some Group members believe that there is an outstanding problem with plutonium swaps and refer the reader to Annexe 2. It is noted that the regulator in this instance is Euratom.				

4. Attributes Relevant to Information Provision

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
4.1	-	See Preamble (Section 4.1)	See 1.1b			
4.2	-	NO IDENTIFIED GAP				
4.3	B	Within the matrix the Group has identified a number of information sources that, if released, would enhance public confidence. There is a public and stakeholder perception of non-disclosure and that information is kept within BNFL. It is recognised that this is a difficult area to benchmark.	BNFL should consider publishing its annual report on security performance, with sensitive details removed.	BNFL	From July 2005	Agreed
4.3	B		BNFL should make its practice consistent with the recommendations that are going forward to the NDA in respect of the presumption of availability of all documentation, with exemptions being determined by criteria set by stakeholders, including OCNS.	BNFL	April 2005	Agreed
4.3	B		Efforts should be made by BNFL to develop a benchmarking system.	BNFL	April 2005	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
4.4	E	The presentation on emergency planning did highlight the difficulties in understanding and communicating events and consequences to the public. Some of the Group members felt that the presentation by Cumbria County Council Chief Emergency Planning Officer failed to reassure them that the pre- and post-incident emergency planning arrangements were adequate for the types of eventualities that some members felt could be a consequence of terrorist activity. Some members of the Group felt that the reference case for the worst credible site accident presented by BNFL and upon which the pre- and post- incident emergency plan is based, and is endorsed by the NII, creates an impression of complacency in light of September 11, 2001. The Group notes that the Chancellor in the latest Comprehensive Spending Review (July 2004) has allocated additional funds to emergency planning and counter-terrorism.	BNFL, OCNS and Nuclear Installations Inspectorate (NII) should re-evaluate the worst case scenario accidents, and the worst case terrorist incidents at its sites resulting in radiation release, in the light of the proposed Joint Fact Finding mentioned above and should undertake to review and rewrite if necessary the emergency plan with relevant local authorities in light of those findings, and communicate it by all media possible.	BNFL	April 2006	Agreed
4.4	A		The adequacy of emergency planning funding arrangements should be reviewed in light of the re-evaluation of the worst case scenario accidents and the worst case terrorist incidents.	Government	April 2006	Agreed
4.5	-	The Group welcomes BNFL's FoIA 'Publications Scheme' but has not yet seen it.				

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
4.6	-	The Group restates that it has not had access to the DBT and therefore is not in a position to know if the system of alert states is responsive to changing circumstances.	See 1.4			
4.7	C	There is still uncertainty about NDA's future stakeholder engagement plans, and BNFL's stakeholder engagement plans post-National Nuclear Dialogue. OCNS has no direct consultation process with a cross-section of stakeholders which creates a problem with respect to information disclosure. The Group notes that the Government did not include any statutory commitment upon the NDA to fund and operate stakeholder dialogue in the Energy Act 2004. The provision of stakeholder engagement is a critical element to a security system.	BNFL and OCNS should put pressure on the embryonic NDA to take on board a commitment to continued stakeholder engagement, embracing the views and opinions of stakeholders generated by the Dti consultation process over the last two years, with particular reference to reforming the LLCs, stakeholder capacity building, and adequate funding. See 1.8.	BNFL Co-ordination Group of BNFL National Stakeholder Dialogue	Now and ongoing	Agreed
4.8	A	OCNS recognises the contrast between the traditional security approach & the openness that the NDA are seeking to demonstrate. OCNS pages on the DTI website are not easily accessible.	The next OCNS report should specifically include a section addressing NDA priorities for security.	OCNS	May/June 2005 (annual report)	Agreed
4.8	B		OCNS should review its openness and transparency policy taking regard to NDA's practices and those of similar security organizations, taking into account FoIA requirements.	OCNS	January 2005	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
4.8	B		BNFL should continue to review its reporting regimes.	BNFL	Annual review from April 2005	Agreed
4.8	G		Consideration should be given by Ministers to formalising parliamentary oversight of civil nuclear security arrangements and the annual report published by OCNS.	Government	July 2005	Agreed
4.8	B		OCNS should set up its own independent website.	OCNS	December 2005	Agreed
4.9	C	Uncertainty over the future and resourcing of stakeholder engagement . There is no mechanism or protocols for reviewing the quality of stakeholder communications to their constituents.	The NDA (and possibly OCNS) should consider how to resource maintenance of links between stakeholders and their constituents, and should bring this issue to the attention of the LLCs or their successors, complemented by dialogue at a national level. Within any future stakeholder process, the NDA should periodically review the quality of stakeholder communication with constituents.	NDA OCNS	Now and ongoing OCNS policy decision by September 2005.	Agreed
4.9	C					
4.10	B	There is currently no requirement on OCNS to brief stakeholders in en route countries. The Group believes this can be undertaken within current intergovernmental arrangements. Some Group members have demonstrated that concerns in en route countries are currently unaddressed: e.g. salvagability of a lost cargo, arrangements of emergency port calls, and environmental impact	OCNS should respond to invitations by foreign states to contribute to the briefing of concerned stakeholder groups in en route countries in connection with international transport of nuclear material. BNFL should promote its willingness to engage with stakeholders in regard to international transport in en route countries, whilst observing diplomatic protocols. UK Government should undertake to address stakeholder concerns regarding salvagability of a lost cargo,	OCNS BNFL Government	Ongoing Ongoing As soon as possible	Agreed

No.	Cat.	Conclusion	Recommendation	Organisation Responsible	Proposed Implementation Timescale	BNFL response
		statement regarding the shipment..	arrangements of emergency port calls, and environmental impact statement regarding the shipment.			

6.0 References

Operation of Euratom Safeguards in 2002; Report from the Commission to the European Parliament and the Council, 2003.

The Anti-Terrorism, Crime and Security Act, 2001.

Assessing the Risk of Terrorist Attacks on Nuclear Facilities, Parliamentary Office of Science and Technology, July 2004.

Annexe 1

Gap Analysis Matrix

1. Overarching Attributes

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
1.1	Make transparently clear at all levels where responsibilities and accountabilities lie, including those relating to the on-going provision of adequate funding. Such transparency should include a clear indication of what the responsibilities are, how they are discharged, what dispute procedures exist and what monitoring systems are available to ensure enforcement.	Regulatory responsibilities rest with OCNS. UK Regulations place clear obligations for security on Nuclear Site Licensees and Company management who are responsible for funding the security measures. BNFL showed the Group detailed charts defining accountabilities for security within the Company. Current funding levels for security are significant but changes in the funding arrangements for NDA-owned sites will affect the way sites are funded in future and the impact of this needs to be considered further. OCNS is responsible for monitoring the implementation of adequate security arrangements & Her Majesty's Inspectorate Constabulary (HMIC) independently reviews the performance of all Police forces, including UKAEAC. Because of its accountabilities, BNFL operates a comprehensive & effective security assurance programme	The Nuclear Industries Security Regulations 2003 (NISR 2003) as a whole are relevant. They require a designated responsible person. The security plan which s/he is required to have approved by OCNS has to show how security will be accomplished, including how it is managed. OCNS evaluates operators' security performance by announced and unannounced inspections.	a. The impact of NDA funding on security from April 2005 needs to be considered further. b. There is no public statement of the security standards that OCNS requires before it approves a security plan. c. NISR 2003 text does not include dispute procedures – operators/ regulators/NDA.	a. The commitment by NDA to fund effective security arrangements, as defined by OCNS, needs to be assured and stated publicly. b. OCNS Disclosure Guidance explains the reasons for this approach (see Appendix 2). c. Make sure Amendment to NISR 2003 includes dispute procedure.	a. No major impact. b. No impact. c. No impact.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		("Diamond") the results of which are reviewed by Executive Directors & action is taken to address any identified deficiencies. The Board of Directors reviews security performance across the BNFL group every year.				
1.2	Make transparently clear at all levels how decisions are arrived at, by whom and against what criteria, and how they may be changed or influenced.	See 1.1 above. In addition, OCNS sets regulatory requirements based on IAEA international guidelines that must be implemented by BNFL. Accountabilities are clearly defined within BNFL. Operators are able to propose security solutions that meet regulations and are able to apply for temporary derogations so long as compensating arrangements are in place. This is subject to formal endorsement by OCNS in advance. Guarding and armed response are provided by UKAEAC.	See 1.1. NISR 2.6 allows for new plans to be submitted. Existing plans cannot be revoked unless there is an approved replacement- OCNS determines the criteria. Some decisions are matters of judgment.	a. A draft Memorandum of Understanding (MoU) is in place between BNFL and the UKAEAC to define accountabilities but this has not been finalised. b. MoU will be classified.	a. Finalise MoU between BNFL & UKAEAC to avoid any mis-understanding over account-abilities and decision-making, including the use of force. b. See OCNS Disclosure Guidance (Appendix 2).	a. No impact - MoU re inter-national transport exists but not on UK sites. b. MoUs in place on certain UK Trans (UKAEAC, Home Office & Scottish Police Forces).
1.3	Ensure that a balance is struck	BNFL has encouraged the open publication of the independent	OCNS aspires to this but it is an unproveable test.	a. Evidence is needed to find out if public and	a. Consider using polls, with careful	Some impact on all 3.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	between the demands of security and the need for transparency to prevent either one undermining the other.	HMIC review of the UKAEA Constabulary - this used to be classified. BNFL is bound by Government Classification Guides on what may be published about the security arrangements but is working proactively with OCNS to review the rules to see if a better balance can be found between secrecy and transparency. BNFL was supportive of the proposal to form a Security Working Group (SWG) within the Stakeholder Dialogue and has been as open as possible with the Group, including a classified briefing on the security arrangements. BNFL has addressed security issues in its first Corporate Social Responsibility Report published in the summer of 2003 and will continue to do this. OCNS has now published two reports on the effectiveness of security in the civil nuclear industry and its third annual report is scheduled for June 2004.	OCNS's primary responsibility is to security, but it is transparent about the way it works. OCNS attempts to draw an appropriate balance between what needs to be secured and what can be put into the public domain. OCNS and BNFL are subject to the Freedom of Information Act (FoI Act), which comes into force in 2005. The FoI Act requires public bodies to disclose official information, subject to specific exemptions including national security, but not on the basis that information is classified.	stakeholder confidence would increase if more information was published. b. FoI Act is as yet untried in relation to security in the nuclear industry and it is not clear whether the rules on disclosure will be successfully challenged by the public.	thought. b. Review the impact of the FoI Act and Disclosure Guidance. The FoI Act should be applied in ways that readdress the question of whether less secrecy will better inform the public and stakeholders as to what the strengths and vulnerabilities of the security systems are.	Further exploration required.
1.4	Recognise and explain that there is no risk-free situation and that the need for	BNFL recognises that there are no risk-free situations and adopts a risk management approach to security based on the DBT. It regularly publishes reminders to	Nuclear industry is required to maintain higher levels of security than any other industry even when the threat is	Unavailability of DBT makes it impossible for external analysis of any gaps.	a. Make sure the DBT is robust, includes as many aspects as possible, is	Impact on MOX & UKTrans, not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	vigilance is constant.	staff and contractors to remain vigilant and encourages the local community to report suspicious events. BNFL has an intranet system available to the majority of employees that provides risk based advice on foreign and domestic travel and a 24 hour emergency service to help any staff or contractors that experience security concerns. It also employs an independent company, Safecall, to help investigate any concerns that staff or contractors may have about security or safety that are not being properly addressed by line management.	low.		dynamic & takes into account as many threateningscenarios as possible. b. Publish as many aspects of the DBT as possible, as in the USA, to increase public and stakeholder confidence. c. Seek to reduce the level of risk/tension by vigilance, but also by trying to understand the views & concerns of adversaries.	
1.5	Recognise that while we must work to reduce the threats to the fullest extent possible we must also anticipate consequences and act accordingly in order to protect public safety and	Reducing the threat is the responsibility of Government and its agencies as well as of BNFL. BNFL is required to have contingency plans for incidents and emergencies that have to be rehearsed as part of the site licence conditions.	Reducing the threat is an important part of HMG's counter terrorist strategy, for example at the political level, direct anti-terrorist activity. However, security is built on the assumption that threat reduction cannot be guaranteed and new	a. Even if there were to be comprehensive planning, there must always be uncertainties about how effective the contingency arrangements will prove to be if faced with a significant	a. BNFL must always be diligent in presenting candid assessments to, for example, policy makers and emergency planners, of the potential hazards	Some impact on MOX, and potentially on UK Trans. No impact on Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	the environment.		threats can arise at any time and without forewarning. Other than occasional anti-nuclear demonstrations, there is very little experience of security incidents that have tested the contingency arrangements for real.	emergency situation. b. The Working Group and Professional Emergency Planners recognise that there are chronically inadequate national resources to deal with a major emergency.	and likely consequences so appropriate planning can ensue b. The Gov. should ensure that it is technically well informed and the appropriate measures are taken to ensure emergency planning is sufficient, & that emergency services cover all significant terrorist threats, e.g. beds to cope with seriously burned casualties.	
1.6	Demonstrate the justification of the security regime in terms of its purpose, legality and compliance with regulations	The security regime is justified on the grounds of the DBT that is defined by Government. The security standards are formal regulations approved by Government and the powers and activities of the Police are	This is covered in the Explanatory note attached to the Regulations.	a. Some of the information necessary to provide justification is sensitive and cannot be made available to all.	a. Ways should be found to provide some information relating to the DBT that provides the public and stakeholders	Impact on MOX & UK Trans, but not Pu

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	and provide a mechanism through which this demonstration could be conducted.	authorised by Parliament. Compliance with the Regulations is independently assessed by OCNS and reported to the Secretary of State in a published annual report. This details occasions that BNFL or its subsidiaries have been directed to improve security or where deficiencies were found by inspectors that required immediate action.		b. The law at the moment is totally insufficient in relation to intruders. There is a tension between the right to demonstrate and the need to protect against unauthorised intruders who might present a terrorist threat.	some means of assessing at least what the minimum protections are against the terrorist threat. US approach of disclosing some elements of the DBT against civilian facilities should be examined b. Examine the law in relation to trespassing at airports, the Channel Tunnel and nuclear installations in other countries.	
1.7	Ensure that an increase in the sophistication or robustness of a security system can demonstrably reduce the risk and that it's	BNFL management and OCNS review security enhancements and expenditure and decisions are taken on the basis of expert judgement rather than any strict application of cost/benefit. BNFL is currently developing a security hazard indicator that may assist	OCNS could not regulate on this basis. While recognising the legitimacy of the desire, there are insufficient examples of attacks against well-protected targets to allow this judgment to be made.	Any increased costs incurred in the improvement in the security system have to be justified against benefits in terms of reduction of threat.	The development of a Security Hazard Indicator would assist in principle in this task and would enable people to see the cost benefit of spend.	Some impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	economically justified on the basis of a cost/benefit analysis.	with the prioritisation of security and decommissioning programmes and associated expenditure.				
1.8	Deliver effective security on the ground, whilst understanding and responding to stakeholder concerns.	BNFL and OCNS consider that the security arrangements are effective and both are participants in the Stakeholder Dialogue and SWG. BNFL welcomes feedback and suggestions from stakeholders and interacts with local community interest groups via the Local Liaison Committees.	Security cannot be absolute but the Regulatory process is designed to ensure effectiveness. Refer to Disclosure Guidance.	There is no formal mechanism for dialogue with a broad cross-section of stakeholders on nuclear security measures.	Develop a formal mechanism.	Impact on MOX, Pu and UK Trans.
1.9	Ensure that the security regulations address the potential misuse and theft of hazardous materials, without impairing their availability for use, and ensure safe management of such materials, including their removal and storage after use.	The security regulations specifically address the issues of sabotage and theft. There is no doubt that the access control measures, vetting requirements and other aspects of the security arrangements, have a significant impact on working practices and reduce the accessibility of nuclear materials.	Regulations cover security against these threats but say nothing about the need to keep materials available for use. It is for the Operator to work that out.	Ideal Attribute is aspirational. You can never have a security system that does not impair operations to some extent. In some circumstances it may be that the economic impact of security measures outweighs the commercial and public viability of the operation.	It would be inappropriate to bridge the gap by allowing commercial concerns to override the need for effective security. The Security Regulations should promote the most effective and efficient security measures consistent with this standard.	Impact on MOX, Pu and UK Trans
1.10	Minimise risk by	Risk assessments are routine	Not a Regulatory	a. The siting of buildings	a. BNFL should	Impacts on

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	careful consideration of siting of plant, building, equipment and transportation operation.	when planning transport operations and security arrangements are intelligence led, aimed at minimising risk. Routes are specifically chosen that avoid high risk areas of the world. In addition to the approved Security Plans, there are other arrangements in place that define the contingency arrangements in the event of a non-security related accident or incident. For marine shipments these are included in the Shipboard Marine Emergency Plan (SMEP). These Plans are specific to each vessel and are approved by the Marine Coastguard Agency (MCA).	requirement as such, but poor siting will either mean that the security plan will not be approved or that more security will be required to minimise the risk. All transport containers are built to internationally agreed safety standards. OCNS is involved in a programme of work to test their resilience against certain specific types of hostile capability and if necessary additional mechanisms for countering these.	on nuclear sites has not, in the past, been determined or significantly influenced by security considerations. b. Absence of a national analysis and strategy for making decisions on the inevitable dynamic tension between continued onsite storage and centralised storage, which involves transport. c. Effective security assumes effective safety measures. Doubts have been raised about the effectiveness of the safety regime when it comes to transport containers. The doubts are based on the current sequential	have formal procedures in place that make an assessment of security implications a prerequisite in its building siting policy. b. Extend BNFL's security hazard indicator to take this into account. This is an important issue for the NDA, in conjunction with Gov depts, to resolve. c. OCNS needs to ensure that the results of the test programme are properly considered by the appropriate safety and security authorities.	MOX & UK Trans.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
				testing system for the resistance of shipping flasks to fire, impact and immersion, which may not simulate the concurrent effects of real life accidents and thus offer less than anticipated protection against the effects of actual attacks.		
1.11	Demonstrate an appropriate state of alert at all times.	States of Alert are based on a well established system in the UK and are assessed by OCNS based on wider Government analysis performed by the Joint Terrorist Assessment Centre (JTAC). Changes of Alert State are communicated to BNFL who rapidly promulgates the information to key personnel by SMS text message. In the event that BNFL was notified of a specific threat that could have off-site consequences, we would do our utmost under the circumstances to warn local residents. Prevention measures would take priority over evacuation in most instances.	OCNS determines the State of Alert: Sellafield tends to attract a higher State of Alert than other nuclear sites. The Security Plan needs to reflect the security measures that will be in place at the different Alert States but the variation is less than at many government sites because even at BLACK (the lowest Alert State) security at nuclear sites is high.	a. Recent events have demonstrated the unavoidable limitations of intelligence assessment. b. Perception that the integrity of the alert	a. It is very important that intelligence information relating to civil nuclear security is not contrived for political purposes. BNFL must be diligent in ensuring that even at the lowest state of alert, security must be adequate to defend an attack that comes without warning.	Impact on MOX & UK Trans, but not on Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
				state is challenged or at risk because it may be being driven by political considerations - not solely by intelligence. c. The public may not understand the meaning of the different states of alert. The definitions are not made publicly available. d. Doubts over whether the local population would be notified should the alert state on a nuclear site be raised to amber or red.	c. Say what the state of alerts mean and their implications on emergency response, at each place they are displayed. Public Info document.	
1.12	Be adequately resourced,	In 2003/4, BNFL and its subsidiaries spent £50 million on operational and capital expenditure related directly to security measures. The Company Executive has never rejected expenditure on security upgrades and its response to the events of 9/11 was exemplary, releasing	OCNS would regard failure to resource security adequately as a failure to comply.	a. As noted in 1.1, the situation post NDA formation needs to be considered.	a. Treasury should be fully briefed on the importance of the continued funding of security arrangements. b. Formal procedure	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		corporate provisions of £20 million to fund additional enhancements. As noted in 1.1, the situation following the creation of the NDA needs to be considered. Decisions will have to be made about priorities for the decommissioning of the NDA owned sites and whether a greater percentage of the available funds should be spent on reducing the potential hazards rather than defending them in perpetuity. OCNS will retain the authority to instruct the site licensees to maintain or increase security related expenditure.		b. There is no formal procedure for determining OCNS resources.	required.	
1.13	Be subject to testing, demonstration and exercise on a rolling basis in order to prove adequacy, improve where necessary, and continue to make relevant to the design of security measures.	See 3.3 - The security testing regime consists of a hierarchical set of exercises that range from table-top to the full involvement of Police & Gov agencies. As explained to the Group by the UKAEAC, the Police conduct routine exercises to test response times & appropriate tactics that would be used in response to potential incidents. In addition to site-based exercises, exercises are also conducted to test the security arrangements and capabilities for marine & road	Some exercises are initiated by the central Government machinery. Live-firing and live-firing simulations are not carried out in the UK partly because this would run risks that would not otherwise be present and partly because they are run with too many artificial constraints. They can also lead to security creep as each side tries to outdo	a. The way in which exercises are currently carried out relies on the UKAEAC to play too many roles. For example, they would take the role of exercise commander, adversary and defence force. b. There are only so many things you can simulate using people, for example it is not	a. BNFL should review whether completely independent personnel should be used as the simulated adversary. b. Advanced computer simulations should be used to	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		movements OCNS has full involvement with the exercise regime and the preparation and design of scenarios. One of the more recent multi-agency exercises was held on the 4th March 2004 and tested the effectiveness of the emergency response arrangements for a security-related incident involving the road transport of a category one package. Participants included BNFL staff and staff of the local Constabulary, UKAEAC, County Fire Service, County Ambulance Service, County Council & Hospital management.	the other. It is important to note that in the UK the prevention of theft or sabotage is not solely predicated on the security authority's ability to kill adversaries on or off site. The UK's approach is to a wholly integrated system of procedural and physical security measures which incorporate an armed response.	feasible to simulate mortar attacks except on military ranges.	enhance the realism and range of scenarios that can be tested.	
1.14	Recognise that transport operations increase vulnerability and require particular measures to compensate.	Compensatory measures to reduce security risk during transport depend on the category of the material being transported but can be generally summarised as: • Minimise time in transit. • Protection of movement information. Consignment details, route and timings. • Vary routes and timings where possible. • Locked vehicles and packages or security approved	Transport Regulations recognise the increased vulnerability. It is essential that security is not compromised, for example by any sense of obligation driven by infrastructure requirements. There are no set response times for incidents in European waters from land based security	Concern remains that transport options are based on infrastructure facilities rather than overall safety and security considerations. The application of different security standards to similar nuclear shipments without explanation causes confusion and concern.	The Group could not agree on a recommendation to take this gap forward but recognise that this could be a topic for future stakeholder engagement. Classified information may be assessed in a two-tier stakeholder dialogue process (see 1.8 above).	Impact on MOX & UK Trans.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		packages. • Civilian escort or travel in convoy. • Vehicle monitoring, communications and tracking with approved contingency plans. • High security vehicles with armed police escort. • Encrypted communications and coded dates used during planning of high security movements. • Threat assessments. • Use of security approved stopping places under controlled conditions. The overall security arrangements need to meet specific criteria in order to be approved and judgements are made about the adequacy of the arrangements, including the level of armed response required. Flexibility is key because security is intelligence led and there is no reason to suppose that exactly the same arrangements need to be used on every occasion.	support because each individual transport is planned according to the security needs of the time.			

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
1.15	Be based on the need to counteract the capability and intentions of the adversary, not on the probability of attack.	The DBT is deterministic in nature, not probabilistic. However, it is important to take into account the potential consequences of a successful attack - successfully stealing plutonium from a plutonium store is much more serious and could have greater consequences than a comparable attack on a store of uranium.	The OCNS approach considers capability (as described in the DBT) only. Adversary intention is not taken into account except to help inform priorities. Thus, for example, protest groups are not seen as a threat of sabotage or theft.	Possible infiltration of legitimate protest group not addressed. See 1.7 above.	More intelligent monitoring of legitimate protest groups.	Impact on MOX & UK Trans.
1.16	Ensure that security measures are integrated into national security and response arrangements.	The contingency plans for BNFL and UKAEAC are integrated into the National arrangements. In the event of a serious security incident involving an armed response, the accountability for directing the incident would pass from the UKAEAC to the Chief Constable of the Region/County & there are formal arrangements in place to effect this transfer of accountability. This transfer of accountability is exercised.	OCNS is fully involved in JTAC's assessments of the threat, and in Government decision making about security measures.			Impact on MOX & UK Trans.
1.17	Make provision for all possible steps to be taken to deny terrorists and other adversaries the	This is a matter for the Government, not BNFL.	The UK Government undertakes a range of active counter-terrorist activities. Nevertheless, the assumption is that			Impact on MOX & UK Trans.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	opportunity to obtain funds, financing and material for operations.		these cannot be guaranteed to be wholly effective and security of valuable assets will always be required.			
1.18	Ensure that the arrangements are comprehensive, effective, and address such measures as the security of IT systems, physical security, personnel security, etc.		All covered explicitly in the Security Regulations. In addition, OCNS works with NII to make sure that safety-critical systems are also secure.	The Regulations governing the security of non-nuclear but radioactive hazards (such as sealed sources) are not as comprehensive, e.g. vetting of drivers.	Bring this to the attention of policy makers in Gov. so that Regulations are consistent, because it has a direct bearing on the public & stakeholder perception of nuclear security. E.g. use armoured vehicles for transport.	Impact on MOX & UK Trans.

2. Attributes Relevant to Regulation

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
2.1	Be transparent, enforceable and capable of generating public confidence.	In the last few years OCNS has published its assessments of the effectiveness of security regulation and operational security standards in the civil nuclear industry. Previously, no such information was in the public domain. OCNS has statutory powers from the Secretary of State, DTI to enforce the security regime.		The level of public confidence in the security regulations is not known.	OCNS should monitor response to all information it puts in the public domain. See 1.3 above (polling).	Impact on MOX, Pu and UK Trans.
2.2	Comply with international, state, regional and local statute.	The UK regulations are fully compliant with international standards.	OCNS takes an active lead in the international community to make sure the international context continues to reflect developments in the threat and how best to protect against it.			Impact on MOX, Pu and UK Trans.
2.3	Generate confidence in the regulatory bodies that they meet their statutory obligations and comprise of demonstrably competent experts and be	This is a matter for OCNS but it is BNFL's perception that OCNS is well regarded by its peer groups. OCNS is resourced predominantly by charges levied on the operating companies. In 2003/4, BNFL was charged over £1 million for regulatory charges relating to inspections and fees to cover the cost of vetting staff and	OCNS recruits its own staff except for the four most senior posts where recruitment is run by DTI. OCNS is resourced predominantly by charges it levies on the operating companies for the work it does.	OCNS independence is based on a Ministerial statement, the strong-mindedness of its senior staff, and the willingness of policy officials to acquiesce in this. The consequence of this is that OCNS can only act on behalf of the Secretary	Comply with Cabinet Office guidelines on best practice regulation, in particular the need for a 'statement of responsibilities'.	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	appropriately resourced.	contractors. This arrangement will continue after the formation of the NDA. OCNS continues to recruit new staff and increase in size.		of State (SoS), not truly independently (unlike NII).		
2.4	Be subject to "independent" review and scrutiny through a transparent mechanism developed with stakeholder input and approval.	This is a matter for OCNS	There is an Advisory Board chaired by DTI and with a representative from the NII, URENCO, and the Security Service.	There is no independent actor on the OCNS Advisory Board, and there is no visibility of the Advisory Board's roles and responsibilities.	Define and establish appropriate governance arrangements for OCNS that include the need for stakeholder input, including a range of perspectives to allow for balanced discussion.	Impact on MOX & UK Trans, but not Pu.
2.5	Be subject to a regulatory system run by regulators who are independent of policy makers, the industry and other vested interests.	OCNS is a fully autonomous department of the DTI entirely independent of BNFL..	OCNS has regulatory and operational autonomy within the DTI (and is entirely independent of BNFL).	See 2.3 and 2.4.		
2.6	Take account of the growing likelihood of litigation should security be breached.	This, to some degree, requires legal accountabilities to be clearly defined, and an assessment made of potential corporate liability.	There is no provision for redress should, for example, OCNS provide inadequate direction to the industry.	Although the Regulator and industry believe accountabilities are clearly defined, it is inevitable that the legal implications of a serious security incident might only become apparent after the	The assessment of corporate liability needs to be conducted.	Impact on MOX & UK Trans, but no Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
				event. It's unclear where, if at all, BNFL's and OCNS's corporate liability currently lies with respect to terrorist incidents. See also 1.2.		

3. Attributes Relevant to Systems

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
3.1	Be designed to encourage and enhance public and stakeholder confidence in the owners and operators and in those responsible for security.	Public and stakeholder confidence can only be properly assessed by seeking their views in a structured, unbiased way, but given that detailed security arrangements are of necessity confidential, it is difficult to see how an objective view can be obtained. We do not know if the public and stakeholders have confidence in the owners and operators with respect to security arrangements. BNFL reports that there has been very positive feedback from US and Russian security professionals that have attended security training workshops at Sellafield. Visiting VIPs and other personnel unconnected with BNFL have been impressed with the arrangements.	The independence of the Regulator is intended to achieve this.	See 1.3, 2.3 & 4.9		Impact on MOX, Pu & UK Trans.
3.2	Involve a robust access control system.	BNFL considers access controls to be robust and are based on defence in depth. Whilst the outer perimeter fence and other fence lines on site are relatively easy to breach, they are designed to alert security response forces to the	This is both a safety Licence Condition (2) and an essential component of the Security Plan. The only specific security measure specified in the	There's always a risk associated with identity management. The debate on this issue is in the public domain.	BNFL should be aware of the latest technology being applied in this area, but should also take into account cost benefits through the	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		unauthorised access and more sensitive areas are further protected by additional access controls. The reaction of the security force is determined by the perceived threat posed by those having accessed the site and is based on using the minimum level of force necessary to prevent criminal acts from taking place.	Regulations is vetting (Reg 9). This is to enable the Regulator to issue directions on new security measures without the time-consuming necessity of changing legislation.		Security Hazard Indicator.	
3.3	Be designed to combat all levels of capability and intention, and flexible enough to respond to perceived levels of threat at any given time.	The system is designed to address the DBT that defines threats and capabilities of potential adversaries that are considered credible in the UK. The DBT is kept under review by OCNS. BNFL is systematically reviewing its security systems against the DBT - this is a complex and time consuming task that identifies those measures that provide defence in depth, performance standards, related accountabilities and targeted ways to test the systems. States of Alert based on the Bikini system are well established in the UK and are assessed by OCNS based on wider Government analysis performed by the Joint Terrorist Assessment Centre (JTAC). Changes of Alert State are	The system is designed to address the DBT that defines threats and capabilities of potential adversaries that are considered credible in the UK. The DBT is kept under continuous review by OCNS and Directives on behalf of the Secretary of State can be made for specific additional measures if necessary. Full flexibility is not possible: some measures such as fencing and access control are capital intensive and need to be fit-for-purpose for several years. Transport infrastructure is a	a. There is a gap between all possible levels of capability including the most unlikely and those threats which are encompassed within the DBT (see Preamble – Section 4.1 of Report). b. Work remains to be done to complete the full analysis in respect of the DBT. There will always be the need for review and adjustment of the systems.	a. OCNS to consider ways of increasing public and stakeholder confidence and understanding of the DBT methodology and of the judgements made, and its continued and immediate relevance to the security climate. b. Requires continued priority and funding.	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		communicated to BNFL that rapidly promulgates the information to key personnel by SMS text message.	necessary given and limits the amount of flexibility that can be built into the system.			
3.4	Ensure thorough and ongoing vetting of staff, contractors and visitors to avoid infiltration of terrorists and other adversaries, and ensure that systems are sufficiently thorough to give high confidence in the identity, credentials and ongoing trustworthiness of personnel, including vulnerability to corruption.	The civil nuclear industry in the UK has a dedicated vetting agency within OCNS that is responsible for vetting staff and contractors and which retains personnel files for all such people. BNFL provided the Group with details of the numbers of people that are vetted at Sellafield and the different types of vetting clearances that are available. All personnel with unescorted access to licensed nuclear sites are required to have their identity and criminal record checked before access is allowed. Further levels of clearance including financial checks and other background information are required before access is allowed to more sensitive locations or where access to sensitive information, technology or nuclear materials is required. BNFL is required to operate an "aftercare" policy to review the continuing suitability of individuals to hold clearance (by confirming this with	Security Regulation 9 stipulates that all staff have to be approved (i.e. security vetted). The vetting level for particularly roles is determined by OCNS. No-one is allowed unescorted access onto a site without a "BC+" (Enhanced Basic Check that confirms identity and criminal record). The processes involved in security clearance are not founded in legislation. Vetting is the subject of regular review to ensure that it remains relevant. The vetting process includes reference to national and international intelligence and law enforcement databases. Vetting is done on a purely	a. Reliability of police records (refer to Bichard Enquiry). b. The law in the UK prevents the vetting agency from providing personal details obtained during the vetting process to the licensees that operate the sites. This means that the licensees are unsighted in respect of possible issues that may relate to individuals that are subsequently employed. It is OCNS that determines whether a clearance is granted but the licensees that subsequently carry the risk of their decision.	b. The companies employing the individuals have sufficient information provided by the vetting agency to manage any potential risk. Vetting agencies could consider making the criteria for vetting available to the companies.	Impact on MOX, Pu & UK Trans.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		line management) and OCNS Investigating Officers conduct periodic security interviews with those that hold higher clearance.	personal basis, regardless of ethnicity, religion, or any other areas of difference.			
3.5	Test the capabilities of the system to defeat the simulated adversary and ensure the tests themselves are realistic and unbiased.	The security testing regime consists of a hierarchical set of exercises that range from table-top to the full involvement of Police and Government agencies. As explained to the SWG by the UKAEAC, the Police conduct routine exercises to test response times and appropriate tactics that would be used in response to potential incidents. In addition to site-based exercises, exercises are also conducted to test the security arrangements and capabilities for marine and road movements. OCNS has full involvement with the exercise regime and the preparation and design of scenarios.	See 1.13	See 1.13 a. There's a limitation to what you can realistically exercise on operational sites or on transport. b. The adversaries are usually played by UKAEAC officers and there could be a tendency for them to employ predictable methods and techniques.	a. Advanced computer simulations should be used to enhance the realism and range of scenarios that can be tested b. BNFL should review whether completely independent personnel should be used as the simulated adversary.	Impact on MOX & UK Trans, but not Pu.
3.6	Accommodate the need for continuous and integrated analysis of the threat and intention level. Information resulting from such	See 3.5 above - the recently formed JTAC performs this function on behalf of the UK Government. OCNS is represented at JTAC and communicates the information to BNFL.	OCNS is a member of the Joint Terrorism Analysis Centre (JTAC) and has access to all terrorist intelligence available to the UK authorities. The information analysis is	See 2.3 & 2.4 No visible or convincing mechanism for holding OCNS to account for its performance, including the dissemination of	OCNS needs a management statement as recommended by the Better Regulation	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	analysis should be made available to all parties concerned with the security of operations.		communicated to relevant parties on a 'need to know' basis. The nature of intelligence means there can never be sufficient of it, and international exchange, whilst good, is inevitably constrained by the internal needs of the countries that own that intelligence.	relevant intelligence.	Taskforce (2003). This could potentially be met by the establishment of an authoritative and independent oversight body.	
3.7	Be subject to a comprehensive performance management system.	BNFL operates an extensive performance management system for security - "Diamond", details of which were described to the SWG. The system is based on the routine reporting and assessment of security performance indicators and any deficiencies are addressed through improvement programmes. An annual report on security performance is provided to the BNFL Board of Directors and, independently, OCNS publishes its own assessment of the effectiveness of security in the civil nuclear industry.	OCNS regards this as a key test of the Security Plan and its operation. The Operator must be able to prove to us that corporate accountability for security is reflected in adequate management arrangements.	Corporate oversight is currently achieved and must be sustained through any proposed future changes within the industry.	Retain strict corporate oversight of security within BNFL.	Impact on MOX & UK Trans, but not Pu.
3.8	Not rely primarily upon secrecy.	Divulging the full security arrangements would compromise the effectiveness of any security	Security has to be pro-active if it is to be known to be effective. You can			Impact on MOX & UK Trans. Pu?

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		regime so secrecy plays an important part in maintaining security in all organisations. However, the security regimes would still be expected to function at some level if completely compromised, depending on the capability and resources of the adversary. In practice, defence in depth means that disclosure of individual systems would not be expected to be critical and would lead to a change in the arrangements as soon as the disclosure became known. We agree that security should not rely primarily on secrecy - for example, it would not be acceptable to transport plutonium in standard vehicles without a security escort in the hope that the secrecy of the transport departure times and route would be sufficient to protect the shipment.	never be sure what your opponent knows. UK security procedures do not rely solely or primarily on secrecy for effectiveness. See also 1.3			
3.9	Above minimum standards, ensure the security in place (including response measures) is not predictable by the adversary.	The security arrangements that are visible to the public, including perimeter access controls and establishing that IT security standards are not being violated, are subject to variation and unpredictability above minimum standards.	OCNS regards this as desirable and looks to Operators to vary their procedures. Searching, for example, varies according to Alert State. But there is a finite limit to the number of security measures. We			Impact on MOX & UK Trans, but not Pu

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
			assume that a determined adversary will take steps to find out - or will make a calculated estimate - about what he might face. Security lies in the strength of the measures not in their predictability and there is an emphasis on the need to have approved tested equipment. This is especially important in those contexts such as transport where unpredictability is difficult to achieve.			
3.10	Contemplate the ending or suspension of a particular activity if the system fails the tests against the adversary's capabilities.	The outcome of security exercises are always the subject of "hot debriefs" and more considered analysis by the Exercise Steering Group that comprises Operators, Police and OCNS. We have not identified any systematic failures of the security regime although there are usually learning points.	No activity can be undertaken unless it complies with the regulations. Decision to suspend or stop particular activities can be taken at a number of levels, including the Regulator and/or the Secretary of State	a. BNFL's security risk assessment methodology does not currently include the results of exercises, though it could and will be in future.	a. BNFL should include the results of security exercises in it's formal risk assessment systems. Vulnerability assessment should be at the level of individual facilities rather than at a more generic site level.	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
					b. The development of a security hazard indicator should be completed as a matter of urgency and it's results used to prioritise decommissioning of potentially hazardous facilities.	
3.11	Guard against cyber-terrorist threats by making computer systems secure against unauthorised interference.	BNFL's computer systems and IT architecture are specifically designed to minimise the possibility of cyber-terrorism. The SWG was briefed on the hierarchy of IT systems and the way in which they are separated to prevent sensitive systems from attack. BNFL has used independent IT consultants for the last 4 years to test the resilience of the systems to hacking (penetration testing). Identified vulnerabilities are actioned for correction	IT systems have to be accredited by OCNS as meeting BS7799. There is separate ongoing work to assess the security requirements of safety-critical IT systems.	Security requirements may be identified and if they are the security regulations will require the operator to implement them.	The Group has been informed that this is addressed on an ongoing basis.	Impact on MOX, Pu & UK Trans.
3.12	Be capable of monitoring communications and infiltrating	This is a matter for Government not BNFL.	Government has a number of strategies aimed at reducing the capabilities of terrorists and other	The public don't know the extent to which these activities take place to reduce the	The Group felt this was outside our remit & this statement covers the	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	terrorist networks to disrupt their modus operandi with the aim of rendering them ineffective.		potential adversaries. There is continuing activity and strong government commitment to doing all that it can to prevent terrorists carrying out their intentions and to reduce the circumstances that lead people to take up terrorism as their only course of action.	circumstances that lead people to terrorism. The Group is aware of the Government publication: Counter-Terrorism Powers: Reconciling Security and Liberty in an Open Society: A Discussion Paper. (Home Office, February 2004), which addresses these concerns. Some members of the Group do not endorse all its solutions.	issue.	
3.13	Be capable of accommodating an independent peer review assessment of consequences in all potentially hazardous facilities and services.	The most recent independent review was by the POST, as a result of a recommendation by the Defence Select Committee. The report was published in July. POST was given considerable access to security information but is only able to reference publicly available information. This introduces an inevitable bias into the conclusions because most official information on the security arrangements and the potential consequences of terrorist action are classified.	Understanding consequence is an important aspect of prioritisation of security.	There are divergent views as to what the consequences are.	Joint Fact Finding approach, possibly initiated and overseen by Local Liaison Committees or their successors, complemented by a dialogue at a national level. This needs to be resourced, and have access to the information.	Impact on MOX & UK Trans, but not Pu.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		Other independent peer reviews have been conducted by Government agencies and have concluded that the security arrangements are effective. BNFL is aware of the concern relating to the consequences of a terrorist attack on the High Active Storage Tanks at Sellafield. We believe that "independent" reviewers have sought to sensationalise the potential consequences without access to accurate information and this has caused unnecessary concern. BNFL has refuted the conclusions because we know that they are based on invalid and exaggerated analyses.				
3.14	Establish security priorities and regimes through a transparent mechanism developed with stakeholder approval and input.	BNFL prioritises security enhancements but this does not involve stakeholders other than regulators and the DTI	The mechanisms for establishing security priorities and regimes are transparent.	There is opaqueness at the moment because the only stakeholders involved are the industry and policy officials.	Ensure that any Joint Fact Finding process involves a greater range of stakeholders to increase public and stakeholder confidence.	Impact on MOX & UK Trans, but not Pu.
3.15	Ensure that only those with an	Given that this attribute requires access to sensitive information to	See 3.2 & 3.4			Impact on MOX, Pu & UK

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	operational need to access sensitive and information can do so, in store, process or transit.	be restricted to those with an "operational need" calls into question the review of this information by a range of stakeholders that have no operational need for the information. The principle of "need to know" is likely to be compromised by a policy of "would like to know".				Trans.
3.16	Be a combination of physical protection, effective safeguards and stock control provide adequate assurance that nothing has gone missing.	BNFL agrees with this attribute. Physical protection is the primary method by which we assure ourselves that material is not removed without proper authority but materials accountancy provides an important complementary measure. In the event that materials- accountancy results identify inventory differences above statistically significant action levels (which is occasionally inevitable in any industrial process), BNFL automatically reviews the relevant security arrangements to establish that theft is not a credible explanation for the difference. BNFL has made significant investment in developing Near Real Time Accountancy systems				Impact on MOX, Pu & UK Trans.

	ATTRIBUTE OF IDEAL SECURITY SYSTEM *SWG view*	**BNFL SECURITY SYSTEM** *BNFL view*	**OCNS REGULATORY PERSPECTIVE** *OCNS view*	**GAP ANALYSIS** *SWG view*	**BRIDGING THE GAP** *SWG view*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		for THORP and other modern plutonium processing facilities that are the best in the world.				

4. Attributes Relevant to Information Provision

	ATTIRBUTE OF IDEAL SECRITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
4.1	Presume that information should be provided but recognise that there exists a need to strike a balance between public trust and risks associated with what is disclosed or withheld within statutory and administrative limits and requirements.	See also 1.3 BNFL has encouraged the open publication of the independent HMIC review of the UKAEA Constabulary - this used to be classified. BNFL is bound by Government regulation on what may be published about the security arrangements but is working proactively with OCNS to review the rules to see if a better balance can be found between secrecy and transparency. BNFL was supportive of the proposal to form a SWG within the Stakeholder Dialogue and has been as open as possible with the Group, including a classified briefing on the security arrangements. BNFL has addressed security issues in its first Corporate Social Responsibility Report published in the summer of 2003 and will continue to do this. OCNS has now published three reports on the effectiveness of security in the civil nuclear industry, most recently in July 2004.	OCNS has published specific guidance on this point in 'Finding the Balance' (2004). It includes the statement "There should be a presumption of openness unless there are cogent and defensible reasons against it".	See Preamble (Section 4.1).		Impact on MOX, Pu & UK Trans.
4.2	Be capable of de-	This is done as a matter of routine.	See 4.1	See 2.1		Impact on

	ATTIRBUTE OF IDEAL SECRITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	sensitising information (reclassified by reducing sensitivity, e.g. omitting certain material) to make it useable to the public and emergency services.		There are standing security instructions requiring holders of classified information to regularly review their material for the current appropriateness of the classification and the retention of the material. There is a UK Classification Working Party whose job is to recommend changes in the requirements to classify information. For example, plutonium production for weapon purposes in the UK was declassified and published as a report in the 1990s.			MOX, Pu & UK Trans.
4.3	Aim at enhancing public confidence in the information disclosure system through the provision of security and emergency response information.	This was what was behind the publication of the information referred to in 1.3 and 4.1. BNFL would welcome suggestions for what additional information the SWG thinks should be published, and to help define the audience and method of publication.	See 4.1 and the annual report of the OCNS.	There is a perception of non-disclosure and that information is kept within BNFL. How do you set a standard against which you can compare and contrast performance in this area? Some of the Group feel it	BNFL should make its practice consistent with the recommendations that are going forward to the NDA in respect of the presumption of availability of all documentation, with	Impact on MOX & UK Trans, but not Pu.

	ATTIRBUTE OF IDEAL SECRITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
				could be possible to develop an agreed definition of documents that would be listed publicly by title with indications as to which are classified in their entirety and therefore not releasable, or sanitized and partially releasable.	exemptions being determined by criteria set by stakeholders (See DTI Stakeholder Engagement).	
4.4	Agree channels for the provision of information (e.g. websites, texting linked to the national network and publications which clearly explain what the emergency response embraces, sirens, points of contact, escape routes, muster points, what to expect, who to ask questions, anticipated flood of calls and requests in the event of an incident which	This information was provided to the SWG.	OCNS requires companies to have an emergency plan as part of their security arrangements.	The presentation on emergency planning did highlight the difficulties in understanding and communicating events and consequences to the public. Some of the Group members felt that the presentation by Cumbria County Council Chief Emergency Planning Officer failed to reassure them that the pre- and post-incident emergency planning arrangements were adequate for the types of eventualities that some members felt could be a consequence of terrorist activity. Some members of the Group felt that the	BNFL, OCNS and NII should re-evaluate the worst case scenario accident, and the worst case terrorist incident resulting in radiation release, in the light of the proposed Joint Fact Finding mentioned above and should undertake to review and rewrite if necessary the emergency plan with Cumbria County Council in light of those findings, and communicate it by all media possible.	Impact on MOX & UK Trans, but not Pu.

	ATTIRBUTE OF IDEAL SECRITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	requires the invoking of the emergency plan).			reference case for the worst credible site accident presented by BNFL and upon which the pre- and post-incident emergency plan is based, and is endorsed by the NII, creates an impression of complacency in light of September 11, 2001.		
4.5	Provide public information in a clear and digestible form.	We try to do this - the CSR Report is one recent example. The Report won an award from ACCA for Best First Time Social Report of 2003. BNFL has produced FoIA "Publications Scheme".	OCNS would like to see information to Operators and to the public in an appropriately understandable form.	Stakeholders have yet to comment on Publications Scheme See 1.3	Stakeholders to comment	Impact on MOX, Pu & UK Trans
4.6	Communicate that the system is responsive to changing circumstances.	The State of Alert system is well established in the UK and is assessed by OCNS based on wider Government analysis performed by the Joint Terrorist Assessment Centre (JTAC). Changes of Alert State are communicated to BNFL that rapidly promulgates the information to key personnel by SMS text message. The DBT is kept under review as indicated in 3.5.	See 1.11 & 3.5	See 1.3, 1.11 & 3.5 a. Most stakeholders are not privy to the content of the DBT.	a. The Group restates that it has not had access to the DBT & therefore is not in a position to know if the system of alert states is responsive to changing	Impact on MOX & UK Trans, but not Pu.

	ATTIRBUTE OF IDEAL SECRITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		In the event that the Alert State increases to Amber or Red, it is not clear whether the local population would be notified. The priority would be to respond to the threat.		b. There are circumstances when the Alert State should be notified to local populations.	circumstances.	
4.7	Put in place structures for rigorous stakeholder consultation. Ensure that body develops and applies criteria relating to what information it is appropriate to withhold.	BNFL has encouraged the formation of the SWG in the Stakeholder Dialogue because it believes that ways should be sought that permit a wider stakeholder involvement with civil nuclear security issues, so long as they do not undermine the security arrangements. BNFL believes that some form of stakeholder engagement should continue.	OCNS has no direct stakeholder consultation process, but has no problem with the operators being involved with it as long as appropriate controls are maintained over information disclosure.	See 4.8 & 4.9 a. Uncertainty about BNFL's future engagement programme, and how NDA's defined engagement programme will work in practice. b. No mechanisms exist for appeals and complaints.	a. In order to provide a high degree of public & stakeholder consultation & to enhance public confidence, should include a Consultative Group comprising stakeholder representatives. b. Mechanisms should also be provided for appeals and complaints.	Impact on MOX, Pu & UK Trans.
4.8	Be flexible in its reporting regime and capable of communicating	In some respects this is linked to 4.5 - our stakeholders include: • staff & contractors - we have established a Help desk that is	This is not what security professionals have traditionally done but OCNS recognises the	a. OCNS recognises the contrast between the traditional security approach & the	a. OCNS report should specifically include a section	Impact on MOX & UK Trans, but not Pu.

	ATTIRBUTE OF IDEAL SECRITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
	different things to different audiences.	available during working hours, an extensive intranet site that covers security matters & provides key briefs, and a 24 hr telephone hotline for all staff & contractors that may experience a security issue whilst travelling anywhere in the world on company business. We monitor internal satisfaction with the services that we provide. • regulators - we provide extensive information to regulators that include formal security plans, assurance statements, etc. We monitor the satisfaction of the regulator with the information that we provide and our attitude to security management. • the public - we would always respond to public queries about security in a courteous & prompt manner (questions arrive by telephone & the BNFL Web site). We have included security issues in BNFL's first CSR Report (see 4.5). • local stakeholders - all sites have local liaison committees • customers - we take a proactive approach to providing	need for it. OCNS now produces a comprehensive annual report to the Secretary of State that is laid before parliament.	openness that the NDA are seeking to demonstrate.	addressing NDA priorities for security. b. OCNS should review its openness and transparency policy taking regard to NDA's practices and those of similar security organisations. c. BNFL should continue to review its reporting regimes. d. Consideration should be given to formalising parliamentary oversight of civil nuclear arrangements and the annual report published by OCNS.	

	ATTIRBUTE OF IDEAL SECRITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
		consultancy services so that we share best practice with other organisations in different parts of the world. We monitor their satisfaction with the services that we provide.		e. OCNS pages on the DTI website are not easily accessible.	e. Set up OCNS's own website.	
4.9	Maintain healthy and viable links between stakeholder representatives and their constituents.	This does not seem to be something that BNFL would have responsibility for but the stakeholder representatives themselves.		a. Uncertainty over the future and resourcing of stakeholder engagement. b. There is no mechanism or protocols for reviewing the quality of stakeholder communications to their constituents	a. Consideration needs to be given to how to resource this activity, and needs to be brought to the attention of NDA & LLCs or their successors, complemented by dialogue at a national level. b. Within any future stakeholder process, need to establish periodic reviews of quality of stakeholder communication with constituents	Impact on MOX, Pu & UK Trans.

	ATTIRBUTE OF IDEAL SECRITY SYSTEM *SWG View*	**BNFL SECURITY SYSTEM** *BNFL View*	**OCNS REGULATORY PERSPECTIVE** *OCNS View*	**GAP ANALYSIS** *SWG View*	**BRIDGING THE GAP** *SWG View*	**IMPACT OF BRIDGING THE GAP ON ToR ISSUES**
4.10	Where trans-frontier shipments of hazardous materials are involved, provision should be made to extend the consultation process to acknowledge and accommodate as appropriate the international dimension.	Nuclear material being transported is always under the operational control and custody of a single organisation and country to avoid confusion and discussions take place ahead of any transport to discuss and agree the formal points of handover. BNFL makes its own efforts to communicate relevant information about international transport to it stakeholders wherever they may be located and routinely deploys international personnel to interface with media representatives etc. We believe that we do far more to communicate this information than any other organisation that is involved with the international transport of potentially hazardous cargoes.	There is no gap in regulatory control as material is transferred from one country's jurisdiction to another. This is an area which is heavily constrained by international law and international jurisdiction issues.	There's no formal arrangement in place to engage stakeholders in other countries potentially effected by the transport of nuclear materials, other than the Governments involved.	We propose that this is redrafted to say OCNS should be encouraged to contribute to the briefing of concerned stakeholder groups in en route countries.	Impact on MOX & UK Trans, but not Pu.

Annexe 2

Plutonium Swaps discussion:

1. Paper by Dr. David Lowry, April 2004
2. Email to the Group from Dave Andrews, June 2004
3. Paper by Dr. Roger Howsley, June 2004
4. Questions about Plutonium Swaps posed to Roger Howsley by Paul Leventhal, July 2004
5. Response to Paul Leventhal's questions, August 2004

1. Paper by Dr. David Lowry, April 2004

Plutonium Swaps

Rationale

The rationale for originally raising this matter in the PuWG was because it was revealed by a BNFL company spokesperson as part of our working group deliberations that at least some of the plutonium used in the fabrication of the MOX fuel assemblies sent to Switzerland came from the BNFL–owned stockpile, rather than from the batch of recovered plutonium arising from the reprocessing of Swiss thermal oxide fuel in Thorp, and held in store on behalf of the customer at Sellafield.

BNFL had therefore substituted its own plutonium for that of a customer in part fulfilment of [what must be assumed, as the company declines to make public the text of any commercial contract, even under the strict ground rules covering confidentiality] to be a contractual commitment to return the reprocessed plutonium to the customer in the form of plutonium (MOX) fuels.

As plutonium from the BNFL-owned stockpile was thus exported, its management and security come under the purview of the Security and Transport Group. The PuWG final report stated the mission for the PuWG was to: “develop and recommend principles for BNFL’s management and reduction of separated plutonium stocks.” (page 11)

Plutonium Swaps

The stockpile of separated foreign customer-owned plutonium at Sellafield totalled 16,700 kgs, with a further 37,000 kgs still in spent fuel to be reprocessed, as at 31 December 2001, according to page 3 of annex 2 of the PuWG report of March 2003. BNFL-owned pu was substituted for a proportion of this stockpile, when the Swiss MOX fuel was fabricated, the exact quantities of which are known to BNFL, but have not yet been shared with the Security and Transport Group. BNFL should certainly make the details available to our group, to allow us to fulfil properly the mission given to us by the Main Group, ie to report on the management and destiny of BNFL-owned plutonium.

Annex 2, page 6 summarises the status and operationalisation of plutonium swaps. It asserts that “the [pu] allocation method….ensures that if the plutonium sent for reprocessing had international obligations attached to it, then these obligations remain with the material provided back to the customer…”
It goes on to record in the subsequent paragraph that such swaps may only be conducted with the approval of the Euratom Supply Agency in accordance with ‘equivalence criteria’ for such arrangements as defined under European legislation. It further asserts that these equivalence criteria are designed to ensure that ‘swaps’ or ‘loans’ fall within ‘comparable fissile content bands’.

Footnote 10 records that “many members of the PuWG are concerned that the details of these criteria are not publicly available and it is not therefore possible to demonstrate that the stated objectives are achieved in practice.”

As of mid-April 2004, this remains the case: it is as unsatisfactory 13 months after the PuWG report was presented to the Main Group of the BNFL Stakeholder Dialogue, as it was at the time.

This practice of fissile material swaps is premised on the principle of 'fungeability', by which the nuclear industry - apparently backed by its safeguards agencies - swaps nuclear materials such as fertile uranium and fissile plutonium for its operational convenience. By doing so it de facto also swaps the 'flags' denoting country of origin of the nuclear material, which were originally attached to allow supplier states to verify end-use commitments.

What is to be done?

- BNFL should provide the STG full details of all swaps undertaken using its plutonium stocks by quantities, dates of swap, pu isotopic composition and countries/utilities involved, along with the safeguards provisions applied to these exports/transports. This information will allow the group to better evaluate how this component of the BNFL-owned separated plutonium stockpile has been managed.

- BNFL should press the European Commission to lift any confidentiality applied to the US/Euratom Nuclear Co-operation Agreement, so that the STG may evaluate the credibility of the assertions as to 'equivalence.'

Dr David Lowry
Stoneleigh

16 April 2004

2. Email to the Group from Dave Andrews, June 2004

Maeve,

Apologies, I should have picked this up at the time. The second note on sheet 34 is correct in saying that the Pu content of Japanese reactor fuel has a higher percentage of Pu 240 than Magnox fuel, but incorrect in saying this makes it more useful for bombs than Magnox fuel. Rather it is the other way around.

The Pu isotopes of main interest to weapon designers are Pu 239 and Pu 240 and in what follows I will ignore other isotopes. A common classification for Pu is as follows :-

Weapon-grade plutonium, containing c. 93% Pu 239 and less than 7% Pu 240.

Fuel-grade plutonium, containing 7 - 19% Pu 240.

Reactor-grade plutonium, containing more than 19% Pu 240.

[Note this classification is used by the US, but the UK does not generally distinguish between fuel-grade and reactor-grade classifying both as reactor-grade.]

Notwithstanding these classifications, however, all grades of Pu can be used in nuclear weapons. All Pu isotopes have critical masses, which means that regardless of the isotopic composition Pu will produce a nuclear explosion if it can be assembled into a supercritical mass fast enough.

According to the OECD/NEA, the percentage of Pu isotopes at discharge in Magnox and PWR reactors is as follows:-

Magnox; 3000 MWd/t burnup - Pu 239 80%, Pu 240 16.9%.
5000 " " - Pu 239 68.5%, Pu 240 25%.

PWR; 33,000 MWd/t burnup - Pu 239 56.6%, Pu 240 23.2%.
43,000 " " - Pu 239 52.5%, Pu 240 24.1%.

[Plutonium Fuel: An Assessment, OECD/NEA, 1989, p30]

Most Magnox fuel has the lower burnup and therefore most of the Pu extracted from it belongs in the category fuel-grade as identified above. The US conducted a nuclear weapon test using such fuel-grade Pu as long ago as 1962. In addition the initial and final fuel discharges from Magnox reactors will likely contain appreciable quantities of weapon-grade Pu because the fuel will have been in the reactor for only a relatively short period.

Publicly available information on the criteria for plutonium swaps seems to be very limited. A report by the Uranium Institute'sTrade Issues Working Group says
"In the case of plutonium, all isotopes are treated equally, that is equivalence on the basis of grams of plutonium." ('SWAPS in the international nuclear fuel market', Uranium Institute, 1996, 2000) For safeguards purposes Pu is also always looked at in terms of the total amount of plutonium involved. Given the % figures quoted for Magnox and PWR plutonium above, it would seem to be the case that the swaps must have to be on the

basis of gram quantities and not isotopic content, since there is no near equivalence between the PU 239 content of each type of fuel.

This casts doubt over the assurance that fuel-grade, or even weapon-grade, plutonium cannot be swapped for reactor-grade plutonium and that swaps are within a relatively narrow % band (as stated on sheets 34 & 35).

Bruno Pellaud, former Head of Safeguards at the IAEA and adviser to the European Commission on EURATOM security matters, wrote recently that "Low burnup fuel contains weapon-usable plutonium that deserves more attention than has been the case so far.....Additional large quantities of weapon-grade and fuel-grade plutonium are contained in spent fuel from gas cooled and heavy water reactors." ['Proliferation Aspects of Plutonium Recycling', Journal of Nuclear Materials Management, Vol XXXI, No. 1, Fall 2002.] (Magnox reactors are gas cooled)

We have obviously not got to the bottom of this issue yet. I would be grateful if you could forward this to SWG members for consideration at the next meeting - which, unfortunately, as previously notified I will not now be able to attend.

In peace, Dave

3. Paper by Dr. Roger Howsley, June 2004

Security, Safeguards and International Affairs

Obligations of supply and exchanges - relevance to security

May 2004

Introduction

The purpose of this paper is to provide information to the Security Working Group on how obligations arise on nuclear material, how exchanges (or swaps) between obligations on different batches of nuclear material are used by the nuclear industry and the relevance to security.

The source of supplier state obligations

A number of countries that supply or process nuclear material (e.g. Canada, USA, Australia), require this material to be tracked throughout the world to give added assurance of peaceful use. Such material is said to be subject to *Supplier State Obligations.* The obligations apply to the nuclear material throughout the nuclear fuel cycle.

Obligations on nuclear material under the control of the European Community are a consequence of international agreements between the Community and third countries or obligations accepted under certain supply contracts. It is the responsibility of Directorate H of the Directorate General for Transport and Energy (DG TREN H) to ensure that the assumed obligations are strictly followed by the European nuclear industry. All nuclear material under safeguards held by BNFL is therefore subject to these requirements. The requirement for reports to be made for material subject to particular safeguards obligations is identified in Article 20 of Commission Regulation (Euratom) No 3227/76.

Within the European Union DG TREN H recognise a number of obligation codes that are attached to nuclear material dependant on which particular safeguards obligations apply. The current obligation codes for reporting to DG TREN H are

Relating to Nuclear Co-operation agreements

Euratom/USA	A
Euratom/Canada	C
Euratom/USA and Euratom/Canada	D
Euratom/Australia	S
Euratom/Australia and Euratom/USA	T

Non-agreement codes

Peaceful Use	P
Not subject to specific safeguards obligations	N

Obligation exchanges

Owners of nuclear material can use obligation exchanges to assist in the management of their nuclear material to ensure that appropriate nuclear material is available in the correct form and location at the right time. Exchanges of obligation can take place between different batches of nuclear material in different locations within the EU subject to approval by DG TREN H.

In particular, obligation exchanges can be used to remove the need for physical transport of nuclear material or to ensure that material in the correct form is available where required. This is best illustrated by an example:

> A utility owns some nuclear material at two different locations, one in the UK and one in Sweden. The material in the UK is Australian obligated and the material in Sweden is US obligated. The utility requires some US obligated material in the UK to meet a particular requirement. Instead of physically transporting the nuclear material from Sweden to the UK it can request to DG TREN H an exchange of obligation between the two batches of material. If approved, the result would be that the utility would then own US obligated nuclear material in the UK and Australian obligated material in Sweden.

This type of exchange has operational benefits to the owner of the material as it avoids costs of transport and associated safety and security arrangements.

Each request for an obligation exchange is treated on a case by case basis by DG TREN H, who assess the request **to ensure that exchanges happen between batches of similar quality or equivalence of nuclear material**. It also refers to the Euratom Supply Agency for the contractual position relating to the exchange. The detailed criteria used by DG TREN H are not available in the public domain, despite requests from BNFL in January 2003 when it asked DG TREN H for an open source reference on the detailed criteria used for obligation exchanges. However the Uranium Institute Report entitled “Swaps in the nuclear fuel market” of 1996 identified the following general procedures:

> *Proposed internal swaps require case-by-case approval by both the Euratom Supply Agency in Brussels (on the contractual and supply aspects involved) and the Euratom Safeguards Directorate in Luxembourg.*

In addition to the principles of equivalence and proportionality, the following are also applied in deciding on the acceptability of a transaction:

- *the proposed swap must facilitate efficient operation of the nuclear industry (economic/industrial justification);*
- *all international undertakings made by the EU must be complied with (includes an analysis of the political aspects);*
- *the contractual situation of the materials proposed for the swap must be in order;*
- *in the case of enriched uranium, the enrichment of the batches proposed for exchange of obligations must be within certain limits;* (NB this applies also for plutonium)
- *the swap must not have the effect of diminishing the quantity of material subject to the most restrictive safeguards undertakings.*

The Euratom Supply Agency, in its Annual Report, publishes information on special fissile material contracts concluded by or notified to the Supply Agency. In this information the number of exchanges is identified each year[3], as shown below:

Year	**Number of transactions**	**Notes**
1990	116	Includes spot contracts, loans and exchanges
1991	123	Includes spot contracts, loans and exchanges
1992	126	Includes spot contracts, loans and exchanges
1993	23	Includes exchanges of ownership, safeguards obligation codes, international safeguards obligation codes and U3O8 against UF6
1994	25	Includes exchanges of ownership, safeguards obligation codes, international safeguards obligation codes and U3O8 against UF6
1995	20	Includes exchanges of ownership, safeguards obligation codes, international safeguards obligation codes and U3O8 against UF6
1996	17	In contrast with previous Annual Reports exchanges of safeguards obligation codes and international exchanges of safeguards obligations are not included
1997	11	Same comment as 1996
1998	6	Same comment as 1996
1999	13	Same comment as 1996
2000	9	Same comment as 1996
2001	4	Same comment as 1996
2002	4	Same comment as 1996

[3] The earlier figures for 1990, 1991 and 1992 included all forms of contracts notified or concurred, whereas in 1993 - 1995 the figures are broken down to different types and only exchanges are included in the table in the report. Then from 1996 onwards it is for exchanges explicitly excluding obligation exchanges. Comparing the 1990, 1991 and 1992 information on all contracts with that for other years gives similar numbers: 2000 - 113 contracts; 2001 - 80 contracts; 2002 - 106 contracts.

BNFL experience of obligation exchanges

It is important to recognise that it is the owners of nuclear material that determine if they wish to exchange the obligation on nuclear material. The role of the operator of facilities (if not the owner of the material) is to confirm the existence of the nuclear material involved in the exchange to DG TREN H and then report the exchange in its accountancy reports to DG TREN H.

Therefore as an operator of facilities and also the owner of nuclear material BNFL has been involved in both applying for exchanges of BNFL owned nuclear material as well as administering the nuclear material accountancy arrangements for exchanges arranged by our customers. Obligation exchanges using BNFL owned nuclear material have been for both uranium and plutonium.

Exchanges on plutonium have occurred between BNFL owned material and plutonium owned by its customers to facilitate manufacture of MOX fuel in the Sellafield MOX Demonstration Facility using plutonium dioxide from the Magnox Reprocessing Plant, rather than from THORP. These were undertaken following appropriate approvals from the European Commission. BNFL wishes to reiterate that the isotopic composition of the exchanged batches were equivalent and were not used as a mechanism for exchanging low and high burn up plutonium[4] batches, that would not in any case have been approved by the European Commission. As noted previously, the isotopic composition of the exchanged batches must be within a narrow range, typically 10%, relative to the plutonium 240 content, e.g. 27% for 30% Pu240, or 24% for 26.4%. Exchanges therefore have no proliferation relevance. BNFL considers it unfortunate that the Commission cannot make the criteria public.

Conclusions

Obligation exchanges can be used by owners of nuclear material to facilitate efficient utilisation of their material, including the avoidance of unnecessary transport between locations. They have no proliferation significance. Approval for obligation exchanges carried out within the European Union is by DG TREN H.

[4] The isotopic values of Magnox and LWR derived plutonium are generally quite similar. The average isotopic composition of plutonium 240 in fuel stored by BNFL from operating Magnox, AGR and LWR stations is 27%, 32% and 24% - i.e. LWR plutonium has the lowest Pu240 content and AGR fuel the highest, with Magnox in the middle. These are average values for civil fuel used for power production.

4. Questions about Plutonium Swaps posed to Roger Howsley by Paul Leventhal, July 2004

Roger,

As promised, here's my question.

Question to BNFL regarding swaps:

A. Has BNFL ever used (or is it prepared to use) swaps as a means of making up a difference between the amount of Pu a customer declares to be contained in a consignment of spent fuel, and a lesser amount of plutonium recovered from reprocessing? In other words, does BNFL substitute Pu from its own stocks to make up a difference between declared and measured plutonium?

B. Is BNFL under contractual obligation to return (in the form of MOX fuel or PU oxide) the amouint of Pu declared by a customer to be contained in spent fuel, or the amount actually recovered from the spent fuel?

C. Aside from the issue of whether swaps are used to make up a shipper/receiver difference, does BNFL report all such differences to EURATOM/IAEA, and are those differences investigated and resolved by the agency to ensure that such differences are not used to mask actual diversion of small but significant quantities of Pu?

Many thanks, Roger.

p.

Roger,

I forgot to include one additional element of the question I just posed about swaps. It has to do with process losses at THORP and how they are made up to fufill BNFL's contractual obligation for the amount of Pu contained in spent fuel. So the question is this.

Betond the issue of making up any difference between the declared and measured amounts of Pu, how does BNFL make up any process losses between what's measured in the dissolver and the amount of Pu oxide recovered at the end of the process stream? Does BNFL make up such losses from its own stock of Pu and how are these accounted for with EURATOM/IAEA. Is there a threshold amount beyond which you have to report a loss? What is that amount?

Thanks again.

p.

5. Response to Paul Leventhal's questions, August 2004

Here are the questions and our answers relating to swaps, that Paul e-mailed a few weeks ago.

A. Has BNFL ever used (or is it prepared to use) swaps as a means of making up a difference between the amount of Pu a customer declares to be contained in a consignment of spent fuel, and a lesser amount of plutonium recovered from reprocessing? In other words, does BNFL substitute Pu from its own stocks to make up a difference between declared and measured plutonium?

We do not use "swaps" for this purpose. The total amount of plutonium allocated is based on the amount actually recovered from the fuel

B. Is BNFL under contractual obligation to return (in the form of MOX fuel or PU oxide) the amount of Pu declared by a customer to be contained in spent fuel, or the amount actually recovered from the spent fuel?

See above - the total amount of plutonium allocated is based on the amount actually recovered from the fuel

C. Aside from the issue of whether swaps are used to make up a shipper/receiver difference, does BNFL report all such differences to EURATOM/IAEA, and are those differences investigated and resolved by the agency to ensure that such differences are not used to mask actual diversion of small but significant quantities of Pu?

We report all shipper/receiver differences to Euratom and the IAEA. The analysis of SRD is but one method that can be used to gain confidence that the safeguards' arrangements are effective.

D. Beyond the issue of making up any difference between the declared and measured amounts of Pu, how does BNFL make up any process losses between what's measured in the dissolver and the amount of Pu oxide recovered at the end of the process stream? Does BNFL make up such losses from its own stock of Pu and how are these accounted for with EURATOM/IAEA. Is there a threshold amount beyond which you have to report a loss? What is that amount?

There are very small process losses for plutonium in the Thorp process. Under the contracts, we allocate a total quantity of plutonium net of process losses, i.e. we do not add back any plutonium to make up for process losses.

Annexe 3

Index of documents circulated within the Security Working Group

Key:

Note:	c*irculated to the Group for their information*
Inform:	*circulated to the Group because it was requested to inform a discussion, or it lead to a discussion*

NB Some documents circulated to the Group, such as notes on the process, draft documents and meeting reports, have not been included.

These documents are available upon request from Maeve O'Keeffe, Stakeholder Involvement Unit, The Environment Council, 212 High Holborn, London, WC1V 7BF (0207 632 0118, maeveo@envcouncil.org.uk), or from the author directly.

Ref No.	Date Circulated	Documents	Provided By	Status
002	06-Mar-03	Note to SSW	David Lowry	note
006	24-Jun-03	Nuclear industries security regulations 2003 - Summary of responses to consultation and conclusions on points raised	David Lowry	note
007	01-Aug-03	OCNS CD: reference documents concerning the security of civil nuclear materials	OCNS	**inform**
008	18-Aug-03	GAO report Jul 03: Spent Nuclear Fuel – Options Exist to Further Enhance Security	Fred Barker	note
009	18-Aug-03	GAO report Jul 03 HIGHLIGHTS: Spent Nuclear Fuel – Options Exist to Further Enhance Security	Fred Barker	note
015	17-Nov-03	Nuclear Risk_Swiss Re report	David Lowry	note
016	18-Nov-03	Nuclear security Statement of the IAEA Director	David Lowry	note
021	28-Nov-03	Report: NEI May 2003 Questionaire with results 5-6-03	Roger Howsley	**inform**
022	28-Nov-03	Paper: Balancing technical and socio-political issues in managing risks_ the radiation perspective	Roger Howsley	**inform**
023	28-Nov-03	Article: Epidemic of fear (Frank Ferudi)	Roger Howsley	**inform**
024	28-Nov-03	Note from David Lowry on Civil Contingencies Bill	David Lowry	**inform**
025	28-Nov-03	Note on Transport of Nuclear Waste	David Lowry	note
026	01-Dec-03	Note on Public Trust	Pete Wilkinson	**inform**
027	08-Dec-03	UCL programme: Managing radioactive waste safely	Grace McGlynn	**inform**
028	09-Dec-03	Article: Dirty Bomb Warheads Disappear	Dave Andrews	note
031	07-Jan-04	Article: Missing Keys At U.S. Nuke Labs	Dave Andrews	note
032	12-Jan-04	CoRWM and West Cumbria	David Lowry	note
033	16-Jan-04	Energy Bill -Lords debate on plutonium management	David Lowry	note
035	23-Jan-04	Emergency packs	Grace McGlynn	**inform**
039	27-Jan-04	Note on Cyber-terrorism	David Lowry	note
040	27-Jan-04	Note on Cyber-terrorism-update	David Lowry	note
042	11-Feb-04	Note on Nuclear Security	David Lowry	note
045	12-Mar-04	Article_Security and Safeguards	Roger Howsley	note
048	06-Apr-04	Note on Counter-terrorism and Nuclear Transport	David Lowry	note
050	08-Apr-04	Article_Security of nuclear sites questioned	David Lowry	note
051	08-Apr-04	Presentation_Shirley Williams_Local Engagement 30.3.04	Roger Howsley	**inform**
052	15-Apr-04	Roger Howsley thank you letter	SWG (via HA)	note
053	16-Apr-04	Note on US documents applicable to UK-Japan plutonium transports	Paul Leventhal	**inform**
053	16-Apr-04	US-Japan Pu security agreements	Paul Leventhal	**inform**
054	16-Apr-04	Note on Nuclear Control Institute documents on Pu sea shipments	Paul Leventhal	**inform**
054	16-Apr-04	Status Report on Sea Shipments of Radioactive Material	Paul Leventhal	**inform**
054	16-Apr-04	NCI Sea Transport Letter to UN Delegations	Paul Leventhal	**inform**
054	16-Apr-04	The Sea Shipment of Radioactive Materials_Safety and Environmental Concerns	Paul Leventhal	**inform**
054	16-Apr-04	A Critique of Physical Protection Standards for Transport of Irradiated Materials	Paul Leventhal	**inform**
054	16-Apr-04	FAQ About Pu MOX Fuel Shipments	Paul Leventhal	**inform**
054	16-Apr-04	Dangers of Shipping Vitrified High Level Waste	Paul Leventhal	**inform**
054	16-Apr-04	NCI Letter to President Clinton	Paul Leventhal	**inform**
054	16-Apr-04	International Law Permits Panama to Prohibit Shipments	Paul Leventhal	**inform**
054	16-Apr-04	NCI Letter to Sec Cohen	Paul Leventhal	**inform**
054	16-Apr-04	NCI Letter to Embassies of 30 En Route Nations	Paul Leventhal	**inform**

Ref No.	Date Circulated	Documents	Provided By	Status
054	16-Apr-04	NCI Press Release_'Gaping Holes' in Legal Barriers	Paul Leventhal	**inform**
054	16-Apr-04	The Need for Further International Action	Paul Leventhal	**inform**
054	16-Apr-04	NCI Letter to Panama Canal Commission	Paul Leventhal	**inform**
054	16-Apr-04	Panama Canal Letter to NCI	Paul Leventhal	**inform**
054	16-Apr-04	Excerpts from Red Team Report	Paul Leventhal	**inform**
054	16-Apr-04	Sea Transport of Vitrified High Level Wastes	Paul Leventhal	**inform**
054	16-Apr-04	NCI Press Release_Coastal States	Paul Leventhal	**inform**
054	16-Apr-04	Legitimacy of Unilateral Actions	Paul Leventhal	**inform**
054	16-Apr-04	Addressing Safety Issues in Sea Transport of Radioactive Materials	Paul Leventhal	**inform**
054	16-Apr-04	Applying the Precautinary Principle to Ocean Shipments of Radioactive Materials	Paul Leventhal	**inform**
054	16-Apr-04	NCI and Green Peace International Press Release	Paul Leventhal	**inform**
054	16-Apr-04	Report by ECO Engineering, Annapolis, Maryland, March 1992	Paul Leventhal	**inform**
055	20-Apr-04	Paper_Plutonium Swaps	David Lowry	**inform**
056	21-Apr-04	Article_Nuclear Flask Safety Fears Allayed	David Lowry	note
057	22-Apr-04	Threat of nuclear terrorism & Sellafield and missing plutonium	David Lowry	note
058	26-Apr-04	Nuclear Materials (Security)	David Lowry	note
059	26-Apr-04	Sellafield Security	David Lowry	note
060	26-Apr-04	POST Nuclear Security Study	David Lowry	note
061	27-Apr-04	Core NCI documents on maritime nuclear transports	Paul Leventhal	**inform**
061	27-Apr-04	Summary Response of the Nuclear Control Institute to Comments on "The Sea Transport of Vitrified High-Level Wastes: Unresolved Safety Issues	Paul Leventhal	**inform**
061	27-Apr-04	Green Peace_NCI Letter to Albright	Paul Leventhal	**inform**
062	27-Apr-04	Threat of nuclear terrorism	David Lowry	note
063	28-Apr-04	Additional core NCI items on MOX transports	Paul Leventhal	**inform**
063	28-Apr-04	Safety Aspects of Unirradiated MOX Fuel Transport	Paul Leventhal	**inform**
063	28-Apr-04	NCI Letter to UK Government on MOX Shipments	Paul Leventhal	**inform**
063	28-Apr-04	UK Government Response to NCI Letter on MOX Shipments	Paul Leventhal	**inform**
063	28-Apr-04	Department of Defense Response to the NCI/Greenpeace Letter	Paul Leventhal	**inform**
063	28-Apr-04	Department of Energy Response to NCI Concerns for MOX Transport	Paul Leventhal	**inform**
064	30-Apr-04	Review of existing arrangements as contained in various security regulations	Pete Wilkinson	**inform**
065	30-Apr-04	Politicians not stakeholders to decide Sellafield future- Dr Cunningham	David Lowry	note
066	02-May-04	RAF Hercules's breach of power station no-fly zone covered up for months	David Lowry	**inform**
067	04-May-04	SMP Update to Security Working Group	Arthur Roberts	**inform**
069	04-May-04	Paper_BNFL IT Policies	Roger Howsley	**inform**
070	13-May-04	SWG photo-report, including: Presentation_Bryan Reeves_Regulation of Transport Security 04.5.04; Presentation_Roger Howsley_Nuclear Security in BNFL 30.3.04; Presentation_Alastair Brown_MOX Fuel Transport Security Considerations & Measures_30.3.04 & 04.5.04	SWG	**inform**
071	06-May-04	EU faces nuclear threat	David Lowry	note
072	06-May-04	What if? Eurpope simulates Qaeda nuclear hit	David Lowry	note

Ref No.	Date Circulated	Documents	Provided By	Status
073	06-May-04	Government orders anti-radiation pills in response to terror threat	David Lowry	note
074	06-May-04	IAEA Report_Severity, probability and risk of accidents during maritime transport of radioactive material	Alastair Brown	**inform**
077	08-May-04	Nuclear Site Guard Force Considered	David Lowry	note
078	08-May-04	Prevent British Energy's nuclear generators falling into the hands of terrorists	David Lowry	note
079	10-May-04	Emergency evacuation at BNFL-operated nuclear plant in US	David Lowry	note
080	10-May-04	Hunt for missing nuclear waste	David Lowry	note
081	10-May-04	Plutonium security problems	David Lowry	note
083	17-May-04	Emails for circulation: 'Two seconds from nuclear disaster'; 'Threat of 'Dirty Bomb' Growing, Officials Say'	David Lowry	note
084	17-May-04	Nuclear Installations: protection against malevolent adversaries	David Lowry	note
086	19-May-04	Radioactive Materials transports across the Channel	David Lowry	note
087	26-May-04	Items for circulation: 'Civil Contingencies Bill' debated in committeee'; 'Keeping Track of Uranium'	David Lowry	note
088	26-May-04	Miller Paper_Are IAEA Safeguards Effective	Paul Leventhal	**inform**
089	27-May-04	Nuclear jet crash 'could kill millions'	David Lowry	note
090	28-May-04	Perception Gap Event Report	Roger Howsley	**inform**
091	02-Jun-04	Emails for circulation: 'U.S. underestimates dirty bombs'; 'Nuclear terrorism is gravest threat to US'	David Lowry	note
092	02-Jun-04	Pu Swaps Discussion (May Photo Report sheets 34 & 35)	Dave Andrews	**inform**
093	03-Jun-04	OCNS Disclosure Guidance	John Reynolds	**inform**
094	04-Jun-04	Emails for circulation: 'Risk of radioactive "dirty bomb" growing'; 'RAF stages `terror strike` on Sellafield'	David Lowry	note
096	07-Jun-04	Press coverage of James Lovelocks warnings	Roger Howsley	**inform**
101	10-Jun-04	Site Reference Accident_Arthur Roberts	Arthur Roberts	**inform**
102	10-Jun-04	Sellafield Reference Accident_David Humphries	David Humphries	**inform**
103	10-Jun-04	Paper_BNFL Response to Pu Swaps Paper	Roger Howsley	**inform**
104	10-Jun-04	Weapons tranfers targeted by UN resolution	David Lowry	note
105	11-Jun-04	Update on FOI fees	David Lowry	**inform**
106	11-Jun-04	BNFL Press Release - Annual Results 2004	Roger Howsley	note
107	21-Jun-04	Managing spent sealed sources	David Lowry	note
108	21-Jun-04	Eigth Report Civil Contingencies Bill	David Lowry	**inform**
110	29-Jun-04	Intelligence and Security Committee, Annual Report 2003-2004	David Lowry	**inform**
111	01-Jul-04	Email_Project Test Framework and Examples	BFWG	**inform**
111	01-Jul-04	LCBL Cover Letter to Main Group June 04	BFWG	**inform**
111	01-Jul-04	Test Framework-Pu-to MG June 04	BFWG	**inform**
112	02-Jul-04	Draft Clause on the setting up of the Cross Sectoral Group1	Neil McCann	**inform**
113	02-Jul-04	Director of Civil Nuclear Security Report 2004	John Reynolds	note
114	05-Jul-04	Sellafield an easy target for hijacked jets	David Lowry	note
118	09-Jul-04	OCNS Appeals procedure	Jan Crispin	**inform**
120	09-Jul-04	Question on Swaps	Paul Leventhal	**inform**
120	09-Jul-04	Additional question on Swaps	Paul Leventhal	**inform**
121	13-Jul-04	PQs: amendment to Energy Bill	David Lowry	note
122	16-Jul-04	CSR details on increased security / counter-terroism expenditure	David Lowry	note

Ref No.	Date Circulated	Documents	Provided By	Status
123	19-Jul-04	POST Report Review	Frank Barnaby	**inform**
124	21-Jul-04	articles & PQs	David Lowry	note
125	21-Jul-04	DBT - UK secret silence whilst US discusses in Congress	David Lowry	note
125	21-Jul-04	GAO report on new DBT	David Lowry	Note
126	21-Jul-04	UK Security Alert Status & Homeland Security Home Page	Rick Nickerson	**inform**
126	21-Jul-04	UK Security Alert Status internet research	Rick Nickerson	**inform**
127	21-Jul-04	UK Security Alert Status	John Reynolds	**inform**
128	21-Jul-04	PQ re MOX shipments	David Lowry	note
129	26-Jul-04	Disclosure Guidance Link	John Reynolds	**inform**
129	26-Jul-04	OCNS Disclosure Guidance_Finding a Balance	John Reynolds	**inform**
130	26-Jul-04	Nuclear plant backed by Blair is £600m 'white elephant'	David Lowry	note
131	29-Jul-04	BBC drama to depict 'dirty bomb' in London	David Lowry	note
132	02-Aug-04	Response to Swaps questions	Roger Howsley	**inform**
133	02-Aug-04	Emails for circulation: 1. Trittin to Boost Nuclear-Plant Protection, FT Deutschland Says 2. New security checks at Norwegian nuclear plants; Nuclear plant considered as target; Sellafield attack could cause widespread cancers; Three accused of leaking nuclear technology released 3. PG&E on hunt for missing nuclear fuel at Eureka plant: Officials hope 4 pounds of radioactive material safely at bottom of storage pool	David Lowry	note
134	05-Aug-04	Emails for circulation: 1. BNFL wants secrecy over movement of radioactive waste 2. U.S. to Keep Reactor Lapses Secret 3. Nuclear Safety Lapses Won't Be Revealed	David Lowry	note
135	05-Aug-04	Some independent views on Sellafield	David Lowry	note
136	06-Aug-04	Energy Act 2004 extract: statutory duty upon NDA regarding stakeholder engagement	Rupert Wilcox-Baker	**inform**
137	12-Aug-04	Sellafield emergency planning competence questioned	David Lowry	note
138	18-Aug-04	Article_Elite armed force stands firm after shake-up	David Lowry	note
139	18-Aug-04	Article_The nuclear shadow	David Lowry	note
140	23-Aug-04	Nuclear materials a terror threat	David Lowry	note
141	01-Sep-04	Emails for circulation: 1. [fantasy] Russian System of State Accounting and Control of Radioactive Material and Waste; 2. Next president may find nuclear threat comes in small packages	David Lowry	note
142	06-Sep-04	New stories on nuclear terrorist threats	David Lowry	note
143	06-Sep-04	'Nuclear Terrorism': Counting Down to the New Armageddon	David Lowry	note
144	10-Sep-04	Emails for circulation: 1. Nuclear Materials (Transport); 2. A target on the Hudson; 3. UK Ships Depart to Pick Up US Plutonium, Sep. 3	David Lowry	note
145	10-Sep-04	New York Nuclear Plant Called Dangerous Terrorist Target	David Lowry	note
146	10-Sep-04	Nuclear security replies in Parliament	David Lowry	note
149	10-Sep-04	BNFL Draft CSR Report: Security and Stakeholder Engagement	Roger Howsley	**inform**
150	17-Sep-04	Review of Nuclear Plant Security Is Faulted	David Lowry	note
151	17-Sep-04	Security Context paper	David Lowry	**inform**

Annexe 4

Security Working Group Membership

SWG Membership – October 2004

Name	Organisation	Rotating chair	Meetings attended								
			24-25 Sep 03	19-20 Nov 03	21-22 Jan 04	30-31 Mar 04	04-05 May 04	08-09 Jun 04	07-08 Jul 04	07-08 Sep 04	11 Nov 04
Dave Andrews	BASIC		✓	✓	✓	✓	✓	×	✓	✓	✓
Frank Barnaby	Oxford Research Group		✓	✓	×	✓	✓	✓	✓	✓	✓
John Charters	GMB		✓	✓	✓	✓	✓	✓	✓	✓	✓
Mike Clark	Irish Sea Nuclear Free Flotilla		✓	✓	✓	✓	✓	×	✓	✓	×
Jan Crispin *	Office for Civil Nuclear Security	John Reynolds	-	-	✓	✓	✓	✓	✓	✓	✓
Roger Howsley	BNFL		✓	✓	✓	✓	✓	✓	✓	✓	✓
Paul Leventhal	Nuclear Control Institute		✓	✓	✓	✓	✓	✓	✓	✓	✓
David Lowry	Independent		✓	✓	×	×	✓	✓	✓	✓	×
Neil McCann	Nuclear Free Future		×	✓	✓	✓	✓	×	✓	✓	✓
Grace McGlynn	BNFL	Rupert Wilcox-Baker	✓	✓	✓	×	*membership withdrawn*	-	-	-	-
Rick Nickerson	KIMO Secretariat		×	✓	✓	✓	✓	×	✓	✓	×
John Reynolds	Office for Civil Nuclear Security	Jan Crispin	✓	✓	✓	×	✓	✓	✓	✓	✓
Arthur Roberts	BNFL		✓	✓	✓	✓	✓	✓	✓	✓	✓
William Waddington	AMICUS		✓	✓	✓	✓	✓	✓	✓	✓	×
Rupert Wilcox-Baker	BNFL	Grace McGlynn	×	×	✓	×	×	×	✓	×	✓
Pete Wilkinson	Wilkinson Environmental Consulting		✓	✓	✓	✓	✓	×	✓	×	✓

* Became member of SWG in January 2004

Annexe 5

Definitions and Acronyms

DEFINITIONS

ADVERSARY	An individual or group desiring to put stakeholders' interests at risk by purposive malevolent act(s). Adversaries with similar approaches may, for planning purposes only, may be considered collectively as **Adversary Types** e.g. Islamist terrorists.
CONSEQUENCE	The level of impact of purposive malevolent acts (or possible acts) on the interests of stakeholders such as the public and those that represent them, the State, key interest groups, and the international community.
CROSS-SECTORAL	Drawn from all legitimate interests. See **Stakeholder**
DEMOCRACY	Government of a State by its people (does not imply any particular process by which that is achieved).
DESIGN BASIS THREAT	The IAEA defines this as the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorised removal of nuclear material or sabotage against which physical protection system is designed and evaluated. The UK extends this definition to include threats to related sensitive information, security measures, and to employees.
DUAL-USE ITEMS	Items that are essential for weapons-use but that have legitimate none-weapons utility.
GAP ANALYSIS	The gap identified between an attribute and the current system as seen.
INTERNATIONAL SAFEGUARDS	The process (operated by the IAEA and Euratom) of accounting for nuclear material to give confidence that nuclear materials used for civil purposes are not being diverted for military use.
MATERIEL	A collective noun, of military origin, for weapons, ammunition, explosives etc.
NUCLEAR MATERIAL	Radioactive materials classified by the IAEA on account of their potential for use in a self-sustaining thermonuclear reaction.
OPERATOR	Operators, licensees, or nuclear material handlers responsible for the physical protection of nuclear material (in use, storage, or transportation) and nuclear facilities. Also those in possession of sensitive nuclear information and subject to regulation as a result.

RISK	The likelihood that a threat will be able to bring about an undesirable consequence.
SAFEGUARDS	See **International Safeguards.**
SAFETY CRITICAL	A feature of a system, particularly an IT system, which meets design criteria for safety purposes but deliberate interference with would prejudice safety provision.
SECURITY	Measures used to manage risk by reducing vulnerability.
SECURITY HAZARD INDICATOR	A measure of security benefit versus implementation cost.
SECURITY SERVICE (MI5)	The Service is responsible for protecting the UK against threats to national security.
SENSITIVE MATERIALS/ SYSTEMS	Anything whose unauthorised loss or damage the owner of the material (or information) would consider undesirable to a greater or lesser degree.
SENSITIVE NUCLEAR INFORMATION	Classified information that could be used to obtain or produce nuclear material.
STAKEHOLDERS	*DTI definition:* i) Groups NDA needs to engage with as a matter of course; ii) groups or individuals with specific knowledge or interest in the issues. *The Environment Council definition:* 'Any party who may have a concern or be a decision maker in the issue. Stakeholders may be i) internal to organisations funding the project; ii) drawn from expert or representative groups; iii) citizens interested in the issues (appropriately in national or local issues)'.
STAKEHOLDER CAPACITY BUILDING	Infrastructure requirements to enable stakeholder dialogue.
STATE of ALERT	A tiered indicator, provided by the Cabinet Office, of the assessed likelihood of hostile activity against a government (mostly) target that triggers tiered security measures for the protection of the target, its employees and visitors.
THREAT	The potential to cause an undesirable consequence.
VULNERABILITY	A feature or weakness that can be exploited by an adversary to bring about an undesirable consequence.

ACRONYMS

BNFL British Nuclear Fuels Ltd.

DBT Design Basis Threat

FoI Act Freedom of Information Act

HMIC Her Majesty's Inspectorate Constabulary

IAEA International Atomic Energy Agency

LLC Local Liaison Committee

MoU Memorandum of Understanding

MOX Mixed Oxide Fuel

NDA Nuclear Decommissioning Agency

NISR 2003 Nuclear Industries Security Regulations 2003

NRC US Nuclear Regulatory Commission

OCNS Office for Civil Nuclear Security

PuWG Plutonium Working Group

SFMOWG Spent Fuels Management Options Working Group

SWG Security Working Group

UKAEAC UK Atomic Energy Agency Constabulary

URENCO Uranium Enrichment Company

Annexe 6

Security Working Group Terms of Reference

Security Working Group – Background and Draft Terms of Reference

Background

Draft work in progress definition of Security:
Applies to the prevention of hostile acts: theft, including technology and equipment, and sabotage

Safeguards and Safety: *will be looked at where they are relevant to the rest of the study, as a full generic study of safety and safeguards is beyond the scope and capability of the group.*

'People are at risk from lapses of security, safety and the failure of safeguards'

The main issues identified by the Main Group and endorsed by the initial meetings of this workstream group for examination are:

- International MOX trade and transport
- Plutonium Swaps
- UK Transport aspects

Openness and Transparency was also identified as a generic factor, and needs to be examined in all the work areas undertaken.

On UK transport, the group would wish to focus on new areas since the main issues have been extensively explored in the dialogue by initiatives such as the Cricklewood dialogue, Jointly Agreed Sampling and Monitoring (JASM), and within Strategic Action Plans (SAP) in Spent Fuel Management Options Working Group and in recommendations from the Plutonium Working Group. These aspects have also been studied outside the dialogue, most recently by the Greater London Authority inquiry. It was suggested, given the time and effort constraints on the proposed group, that transport aspects might focus most usefully on legacy waste management.

On MOX transport, the group proposes to cover the issues raised in the Plutonium Working Group Report, and will undertake any recommendations within its remit from other working groups.

Proposed Methodology

It is suggested that the issues identified above should first be put into context by studying for security;

- The attributes of an ideal system
- The attributes of the current system, *which should identify*
- Areas requiring further examination, which could form packages of a future work programme, either within the BNFL Dialogue or as recommendations to other agencies such as OCNS and DTI.

Both the generic and the particular studies would facilitate a gap analysis, which should lead to recommendations to BNFL and other relevant bodies, for example OCNS.

The work programme should be completed by summer 2004, with a report to a Main Group in the Autumn of that year.

The group, which could be called the Security Working Group, recommends that it is formed as a separate working group, but with close links to BFWG assured by a significant continued cross-representation. In order to be established within the ground rules, the group membership needs to be examined against the need for representation across a wide range of constituencies.

The group envisages consulting a range of external experts who will be determined as necessary.

Appendix 1

POST note and review of full report

1. POST note: Assessing the Risk of Terrorist Attacks on Nuclear Facilities, Parliamentary Office of Science and Technology, July 2004
2. Review of POST report by Frank Barnaby

July 2004 Number 222

TERRORIST ATTACKS ON NUCLEAR FACILITIES

In recent years there has been increased awareness of the risk of terrorist attacks on nuclear facilities, which could have widespread consequences for the environment and for public health. This POST note is a summary of a longer report on this issue, which has been prepared by POST, following a request from the House of Commons Defence Select Committee in July 2002 in its report on *Defence and Security in the UK*.

Background

POST's report aims to provide Parliamentarians with an overview of what is publicly known about the risk of sabotage of nuclear facilities[i] by terrorists. It begins by outlining what is known about the four stages involved in assessing the risk of sabotage:

- **Intelligence**: assessing the nature of the threat.
- **Vulnerability**: assessing the physical robustness of nuclear facilities.
- **Security**: assessing the resilience of security regimes.
- **Consequences**: evaluating the impact of an attack.

Four issues are then discussed in more detail: the operation of nuclear power plants; reprocessing plants; transport of radioactive material and emergency planning.

Limitations of POST's report

Since the report only contains information in the public domain, it is necessarily constrained because much of the information required to provide a comprehensive analysis is classified.[ii] POST's report does not make recommendations. The aim is to summarise current information and to place the diverse commentary on this issue in context.

Types of nuclear activity

Commercial nuclear power gives rise to most of the UK's total radioactive inventory, of which the largest amounts are at the Sellafield reprocessing plant in Cumbria, and at Dounreay in Scotland, the site of earlier research and reprocessing activities. There are also 13 generating power plants, 6 decommissioning power plants and various other military and civilian sites across the country. The closest overseas sites are six power plants and a reprocessing plant in Northern France and two power plants in Belgium. Smaller quantities of radioactive material are used in medicine, industry and research. Most of these activities also involve transport.

Intelligence information

Although awareness of the terrorist threat to nuclear facilities existed before September 11th 2001, the threat to a wide range of facilities, including nuclear, has since been re-evaluated. Information on the type of attacks for which UK civil nuclear sites must be prepared is contained in a classified document, the Design Basis Threat (DBT). This is drawn up by the Office for Civil Nuclear Security (OCNS), based on intelligence information about potential attackers.[iii] In recent years public attention has focussed on the risk of aircraft impact, but OCNS points out that other modes of attack are also considered, such as attacks involving vehicles loaded with explosives, or suicide bombers. The prevention of non ground-based attacks, such as aircraft impact, is seen as Government's responsibility, although site operators might be expected to take mitigating or preventative measures.

Physical robustness of nuclear plants

The full report describes how safety measures incorporated at the design stage and during the operation of UK nuclear facilities can, in some cases, increase robustness to deliberate acts. One of the most important principles on which modern nuclear plants are based is defence in depth, whereby several different systems perform the same function, so that the safety of the plant does not rely on any single feature. All facilities must comply with the requirements of the UK nuclear safety licensing regime, but more modern facilities have more extensive safety provisions. Under the licensing regime, nuclear facilities must be designed and operated to cope with a variety of accidents predicted in the plant 'safety case'. The safety case itself is not required to take a deliberate attack into consideration. The range of accidents with which plants must be designed to cope, has been decided on the basis of their predicted *accidental* likelihood as well as the severity of their outcome. However, calculations of accidental likelihood are not relevant for terrorist acts.
For nuclear installations constructed over the last 10 years, security considerations have been incorporated at the design stage and are part of the regulatory requirement. Security considerations have not been specifically taken into account in the design of some older UK civilian nuclear installations (e.g. power plants), which have had additional security features retrofitted.

Security regimes at nuclear sites

Numerous off-site counter terrorist activities take place to prevent terrorist attacks from being launched. These include intelligence gathering; surveillance of suspect individuals and taking measures at airports to detect and prevent hijackers. However, if terrorists did succeed in launching an attack on a nuclear facility, they would have to overcome the security regime in place at the facility itself. A combination of security measures are in place, designed either to stop attackers or to detect and contain them until an armed response is able to intervene. According to the principle of 'defence in depth', such systems consist of interlocking personnel, procedural, physical and technical security systems so that damage to any one component of the system should not result in a security breach. Security regimes also address other threats including the theft of proliferation sensitive technology.

It is difficult to assess the resilience of security regimes based on public domain information. The UK carries out some practical exercises to test regimes at civilian nuclear sites but details are classified. Greenpeace has breached security twice at the Sizewell B power station and states that this shows the security regime could not withstand an attack. However, according to OCNS these breaches '*would not have provided a viable means for terrorists to penetrate sensitive inner areas'.*

Recent legislation

The full report describes how security at nuclear sites in the UK and overseas has been reviewed since September 11th 2001. For example, public access has been greatly restricted and some information previously in the public domain has been withdrawn. The UK Nuclear Industries Security Regulations 2003 enabled the introduction of measures to strengthen UK civilian nuclear security regimes, described in more detail in the full report.

Guarding of sites

UK law does not permit sites to be protected by armed civilian guards. Certain civilian nuclear sites (including Sellafield and Dounreay) are protected by on-site armed police of the United Kingdom Atomic Energy Authority (UKAEA) constabulary. Other sites (including

nuclear power stations) are currently protected by on-site unarmed civilian guards. Since the jurisidication of the UKAEA has recently been extended, arrangements have been made to provide mobile cover while consideration is given to stationing armed police at these sites.

Evaluating the consequences of an attack

The consequences of a successful attack on a nuclear facility would depend on:-
The size and nature of the release, known as the 'source term'. This would in turn depend on factors such as the extent of the damage and the physical and chemical properties of the materials released.
The movement of radioactive material through the environment and its uptake by the human body. Weather conditions would greatly influence the distribution of radioactive material.
The efficiency of countermeasures put in place to protect people from radiation, e.g. restricting food and water supplies, sheltering, or evacuation. The area over which environmental decontamination measures were implemented would also be a key factor.

Regulation requires UK operators of nuclear licensed sites to evaluate the health and environmental impacts of accidental releases of radioactive material. In general these reports are not publicly available, although considerable information is available from the Sizewell B and Hinkley Point C public inquiries.

Attacks on specific facilities

Commercial power plants

Types of attack

The core of a nuclear reactor in a power plant contains over 100 tonnes of radioactive material at several hundred degrees Celsius. Its safety therefore relies on controlling the nuclear chain reaction, cooling the reactor core and containing the radioactive material. Terrorists might attempt to cause a release in two ways:

- Directly: reactor cores are protected by thick concrete shields, so breaching the reactor containment and shielding would require a violent impact or explosion.
- Indirectly: A release might occur if enough critical safety systems were damaged, but because of defence in depth, this would require a high degree of access, co-ordination and detailed plant knowledge.

Most published commentary focuses on the first possibility, particularly on aircraft impact. Different studies, discussed in more detail in the full report, draw different conclusions depending on the facility in question, the type of aircraft, and its speed and angle of approach. For example, studies carried out for the Sizewell B public inquiry conclude that, in a worst case scenario, if a military aircraft were to strike the reactor building, there would be a 3-4% chance of uncontrolled release of radioactive material. The US Nuclear Energy Institute rule out breach of a US style reactor containment by large commercial aircraft, on the grounds that an aircraft would be unlikely to strike at the angles and speeds necessary to cause sufficient damage.[iv]

Power plants in the UK

The UK currently has three types of commercial reactor:

- 'First generation' Magnox gas cooled reactors. There are 12 reactors operating in 5 power plants.
- 'Second generation' Advanced Gas Cooled reactors (AGRs) of which there are 14 reactors at 7 plants.
- 'Third generation' pressurised water reactor (PWR). There is only one PWR, at Sizewell B in Suffolk.

Because of specific design features the UK's three oldest Magnox reactors (all of which are currently scheduled to cease operating by 2006) may be more likely to sustain physical damage than other UK reactors, in the event of an attack. However, more detailed studies would be necessary to draw more general conclusions on the relative vulnerabilities of gas-cooled reactors and PWRs.

Consequences of a release from a power plant

In the event of a release, radioactive iodine and caesium, dispersed over wide areas, would probably make the most significant contribution to the radiation exposure of the general public. Radioactive iodine can increase the risk of thyroid cancer, particularly in children. It poses a threat mainly in the first few weeks after a release. Radioactive caesium concentrates in topsoil and can be absorbed by plants and so enter the food chain. It can pose a risk for hundreds of years. Following Chernobyl (see box below), levels of radioactivity from caesium deposition led to food related countermeasures in most European countries.

Accidents at civilian nuclear power plants

The two most serious accidents at civilian nuclear power plants to date are the Chernobyl accident in 1985 and the Three Mile Island accident in 1979. At Chernobyl, where there was no effective containment structure around the reactor core, roughly half of the reactor's iodine inventory and one third of the caesium inventory was released. 134 workers suffered acute radiation sickness and 28 died within three months. The main long term effect seen to date is an increase in thyroid cancers in children exposed to fallout.[v] Over 300,000 people were resettled and the financial costs have run to hundreds of billions of pounds. However, at Three Mile Island, most of the release was contained within the reactor building. Negligible amounts of radioactive material were released into the environment and there are no established radiological health effects from the accident.

The amount of material released would vary depending on the extent of the damage, the type of reactor and its operating state. There is inherent uncertainty involved in predicting the size of a release. For example, published studies of potential accident scenarios at Sizewell B, carried out by the National Radiological Protection Board in the 1980s, indicate that if the reactor core were severely damaged, the fraction of radioactive iodine released would vary widely depending on the cause of the damage and the resulting sequence of events. In the majority of cases, less than 0.003% would be released, but the release fraction could exceed 50% (comparable with Chernobyl) in certain very extreme scenarios.

Used fuel storage

Used reactor fuel is mainly stored in cooling ponds under several metres of water. Storage takes place both at reactor sites and reprocessing plants. The main mechanism by which large releases of radioactive material could occur is by loss of cooling water. This might result in overheating and damage to fuel elements, releasing radioactive material into the atmosphere. Loss of cooling could be brought about by direct breach of the ponds and surrounding shielding (e.g. by aircraft impact). There is conflicting commentary on the feasibility of such an attack, the likely release size and the time available to take remedial

action. The full report discusses how these factors depend on the mode of attack, the design of the facility, and the type of fuel in storage.

Attacks during transport

The full report discusses the risks associated with a range of different types of shipment of radioactive material, focussing on the transport of used fuel from power plants, which accounts for the bulk of the radioactive inventory transported each year. Many analysts suggest that an attack on a road or rail shipment of radioactive material might be easier to accomplish than at a fixed installation, and could take place near major population centres. However, the amounts of material involved are smaller and published studies indicate that material would probably be dispersed over a smaller area**.**

Reprocessing plants

Reprocessing plants extract re-usable uranium and plutonium from used reactor fuel and handle a range of radioactive materials. Public attention focuses on the storage of high level liquid radioactive waste (HLLW), plutonium and used reactor fuel, due to the the size of the radioactive inventories involved and (in the case of HLLW and plutonium) their physical state. Published commentary on the potential consequences of releases of radioactive material from these facilities is reviewed in the full report.

High level liquid waste (HLLW) at Sellafield

The largest inventories are at Sellafield, with smaller quantities in storage at Dounreay in Scotland and Cap de la Hague in France. As of July 2004 there are between 1000-1500 cubic metres of HLLW in storage at Sellafield. Certain radioactive isotopes are present in quantities several hundred times greater than in a typical reactor core**.** Although temperatures are far below those in a reactor core, HLLW requires constant cooling to keep it in a safe state. It is stored in tanks awaiting conversion to a more stable form. As with a nuclear reactor, a release might come about directly, through breach of the containment and bulk shielding around the tanks, or indirectly, by prolongued damage to cooling systems. Reports in the public domain assume varying release sizes, from 1/10,000 of the contents of one tank, to over 10% of the total inventory. However, there is insufficient published information on the *likelihood* of different release sizes to judge how realistic these assumptions are. The latter is a 'worst case scenario' assumed to result from a violent impact (e.g. an aircraft) or internal explosion. Published analyses, discussed in more detail in the full report, suggest that *if* a release of the latter proportions were to occur, it could result in hundreds of thousands of long term cancers (assuming some countermeasures were imposed). BNFL[vi] considers these conclusions to be unsubstantiated, on the grounds that *none of the authors have access to current engineering and construction information necessary to undertake a credible study.* BNFL has also stated that it '*does not believe that the physical effects of an aircraft impact upon this building would result in a loss of bulk shielding or containmen*t' on the basis of confidential impact studies.

Plutonium at reprocessing plants

The reprocessing plants at Sellafield and Cap de la Hague store separated plutonium in the form of powdered plutonium oxide. There are few published reports evaluating the impact of sabotage of a plutonium storage facility. In a worst case scenario this could result in atmospheric dispersal of particles containing plutonium, in a fire or explosion. If these particles were small enough to be inhaled, people would have an increased risk of developing lung cancer. BNFL recently constructed a protective wall around the plutonium storage facility at Sellafield.

Long term management of radioactive waste
There is currently no long term management strategy for the UK's intermediate and high level radioactive waste. In 2003 the Government set up the Committee on Radioactive Waste Management (CoRWM) to advise on strategies. CoRWM anticipate presenting final recommendations to Ministers in late 2006. Options include deep geological disposal or storage, which many commentators believe provides better protection from terrorist attack than surface storage.[vii]

Emergency planning
Existing measures to protect the public in the event of accidental releases would also be called upon if there were a deliberate attack. In the UK, detailed off-site plans are in place within a few kilometres of nuclear sites which are designed to be extendible to 10-15 km if necessary. However, some analysts believe that the UK should strengthen arrangements for dealing with releases which could affect wider areas.[viii] The full report discusses a range of issues raised in published commentary, relating to existing emergency planning arrangements. It also discusses the Civil Contingencies Bill, which aims to increase UK resilience to emergency situations.

Overview
There is sufficient information in the public domain to identify ways terrorists might bring about a release of radioactive material from a nuclear facility, but not to draw conclusions on the likelihood of a successful attack, or the size and nature of any release.

There are few detailed published assessments of the physical robustness of nuclear facilities to terrorist attack. Those carried out by the nuclear operators are usually classified and although they are subject to regulatory scrutiny, they are not subject to a public peer review process due to their sensitivity.

Nuclear power plants were not designed to withstand attacks such as large aircraft impact, but existing safety and security regimes provide some defence.

Published reports draw widely different conclusions about the consequences of attacks on nuclear facilities, due to differing assumptions about the size and nature of the release, weather conditions and efficiency of countermeasures.

Reports have been published which suggest that in a worst case scenario, the impact of large aircraft on certain facilities could cause a significant release of radioactive material. Some analysts argue that accurately targeting these facilities would be difficult.

A successful attack would be highly unlikely to cause large numbers of instant fatalities. Although it would have the potential to affect extensive areas of land and cause large numbers of long-term cancers, its impact would depend on how effectively appropriate contingency plans were implemented.

Even an unsuccessful attack could have economic and social repercussions and affect public confidence in nuclear activities such as power generation.
While there is a framework for quantifying the likelihood of accidental releases of radioactive material from nuclear facilities, it is not possible to acccurately assess the

likelihood of a terrorist act as this depends on factors such as terrorist intentions and capabilities.[5]

[5] For the purposes of POST's report the term 'nuclear facility' is also used to refer to shipments of radioactive material.

[2] The UK nuclear operators, regulators and other official bodies have assisted POST by providing staff with access to sensitive inner areas at Sellafield and with classified background briefings.

[3] The Office for Civil Nuclear Security within the DTI is the UK's civil nuclear security regulator.

[4] The US Nuclear Energy Institute is the policy organisation of the nuclear energy and technologies industry in the US.

[5] *Exposures and effects of the Chernobyl accident,* United Nations Scientific Committee on the Effects of Atomic Radiation, 2000

[6] British Nuclear Fuels plc.

[7] *Managing Radioactive Waste: the Government's consultation,* House of Lords Science and Technology Committee, 2001-2002.

[8] *Local Authority Emergency Planning in the locality of UK nuclear power plants,* Large and Associates, 2002.

2. Review of POST report: *"Risks and consequences of terrorist attacks on nuclear facilities", by Frank Barnaby*

The confidential draft report of the Parliamentary Office of Science and Technology (POST) entitled "Risks and consequences of terrorist attacks on nuclear facilities" (working title) is at least 147 pages long. It contains a large amount of very useful information. But it is: short on critical analysis; written in very careful, diplomatic language; and has few recommendations. Recommendations are not part of the remit of POST.

The report draws a number of conclusions. Although there is sufficient public information available to identify possible ways terrorists might bring about a release of radioactive material from the facilities examined in the report there is not enough information to draw definitive conclusions on the likelihood of a successful attack, or the size and effects of any release. Throughout the report there are comments on a lack of information; the authors are obviously frustrated by this lack.

It also concludes that the uncertainty in the likely size of a release gives rise to a wide range of reports in the public domain. For example, some reports predict several million fatalities in the event of a successful attack on the high level waste tanks at Sellafield. These figures are based on assumptions that over half of the radioactive inventory of the tanks could be released in a successful attack. It not possible, it says, to assess these analyses 'in context'. BNFL state that they do not consider the scenario to be credible and argue that such "release estimates have never been justified or underpinned".

According to the report: "Public concern has focussed mainly on facilities which house large inventories of radioactive material in a dispersible form. However these facilities generally have high levels of protection compared with other facilities with smaller inventories. An attack on a 'softer' target could still cause widespread panic and disruption."

Detailed emergency plans are in place for areas within a few kilometres of nuclear sites and could be extended to tens of kilometres if necessary. However many analysts argue that the UK should have more robust plans in place to deal with larger releases of radioactive material which could affect a wider area (e.g. of the scale seen during Chernobyl).

The nuclear authorities, the report explains, face an inevitable conflict between the need to protect sensitive information, and the need to keep the public informed. The events of 9/11 "severely constrained the efforts of many organisations, for example the Nuclear Installations Inspectorate, to be more open about their activities. There is insufficient information for a member of the public to make an informed decision about the level of the threat faced from potential terrorist attacks at nuclear facilities. Thus a very high level of confidence must be placed in the regulators".

It points out that: "There are few detailed assessments of the physical robustness of nuclear facilities to terrorist attack. Assessments carried out by the nuclear operators are usually classified and are not subject to a public peer review process due to their sensitivity. If a detailed assessment were to be carried out based on publicly available information, a range of assumptions would have to be made about the design of the facility. Moreover, it would not be easy to put the results in context without some understanding of terrorist intentions and capabilities. Also, it is not the government's policy to comment on security issues, so there would be no response to such a study."

Appendix 2

OCNS 'Finding the Balance' Document

NB The latest version of this document is obtainable at www.dti.gov.uk/energy/nuclear/safety/disclosure_guidance.pdf

FINDING A BALANCE

GUIDANCE ON THE SENSITIVITY
OF NUCLEAR AND RELATED INFORMATION AND ITS DISCLOSURE

Issued by:

The Office for Civil Nuclear Security
Department of Trade and Industry
B146 Harwell
Didcot
Oxon OX11 0RA

Draft Version 08

May 2004

CONTENTS

PREFACE

There are many official sources of information about civil nuclear materials and facilities. Following the terrorist acts in New York and Washington on 11 September 2001, concern was expressed in various quarters about the amount of information that was so publicly and easily available to terrorists. There was increased awareness that the ease with which such information could be obtained made it easier for terrorists and others to make their plans without taking any risks. It was recognised that the benefits of a culture of openness were accompanied by risks.

There is a considerable body of legislation that requires disclosure of information for a variety of purposes. Some of these are official purposes to do with planning, environmental protection etc. Others are to do with public information and consent. The purpose of this document is to assist officials and others involved with the civil nuclear industry to reduce the risks associated with compliance with their legal obligations. It is not intended in any way to water down those legal obligations only to help, if possible, lessen the ease with which those with malevolent intent can obtain the information they need.

In support of the Government's desire for transparency, this Guide carries no protective marking. It may seem paradoxical to identify publicly the types of information that could be used by terrorists. But the balance of advantage is in increasing awareness. In any case, there is nothing sensitive about, for example, stating that information about the quantities and whereabouts of plutonium is sensitive. It is the actual information that is sensitive. It may not be possible to protect the information totally but the purpose of this Guide is to help readers think about it. Is it, for example, necessary on all plans to identify a plutonium store or only on those plans used by those with an operational reason for knowing? And is it possible for these plans to be labelled as sensitive and given some protection? The answers may be negative but the issue requires thought.

A considerable amount of such information is already easily available. There is no way of recalling it. Details do, however, change. Often they change over quite short periods of time. Published information becomes unreliable if it is not regularly updated. One purpose of this guide is to begin that process. The guide, although published by the Office for Civil Nuclear Security (OCNS) as part of its remit, has been produced after widespread consultation with the industry, government departments and agencies, and the devolved administrations. It must be understood that this document provides *guidance* only. It is not a statutory instrument and has no force in law. However, further guidance should be sought from the appropriate department/authorities if a statutory requirement to release information seems at variance with this guide.

No document of this nature can be completely definitive and cases may arise where it provides little or no help. It is intended to be a dynamic document and may be amended through experience. As with any information covered by the FOI Acts and other Regulations, a decision not to disclose that is based on this guide may be open to challenge. Any such challenge will be dealt with on a case-by-case basis. OCNS believes, however, that a decision not to disclose that draws on the sensible use of this guide is more likely to be upheld.

The Ministry of Defence has a number of Guides concerning the protection of information related to the security of material used in the nuclear weapon and nuclear propulsion programmes. These programmes are outside the scope of this Guide.

PART 1

WHAT IS THE PROBLEM?

If nuclear material were to be stolen or sabotaged, for example by terrorists, the potential consequences could be extremely grave. Nuclear material, its transport, and the processes in which it is used for civil purposes - principally power generation - need to be well protected. In the United Kingdom, a high level of security is expected at nuclear sites and there is a strict process of regulatory enforcement by the Office for Civil Nuclear Security. An important aspect of this security is the protection of information about civil nuclear material and operations and, of course, information about security measures. However, such knowledge and information is also a necessary, often essential, part of running the business. Some information may need to be available to a large number of people. Not all of these are part of the industry e.g. planners, police etc. Members of the public may also have a legitimate interest in information about nuclear facilities and operations.

The problem is how to reconcile these apparently conflicting requirements. How can information be made available to those who need it whilst keeping it from those who could take advantage of it for their own malign ends?

Few would advocate total openness of all nuclear related information. But if some knowledge is to be restricted, how do you decide what that is, to whom it should be restricted, and how do you ensure that they are able to keep it secure? Not all organisations need high levels of security for the rest of their business. When a large number of people need to know something in order to carry out their job, the knowledge is hardly a secret even though it could be misused. Neither total openness nor total security are viable options.

WHAT CAN BE DONE?

Some of the obligations about disclosure are described in Annex A. In a situation of conflicting demands and interests, a single overriding solution is unlikely to be available. In any case, situations rarely remain static. Information that is not required one day, may be required the next. Case-by-case judgments are often required. Are the risks of not disclosing something greater or less than the harm occasioned by disclosing it? Knowing why to disclose something is usually easy. But there may be little or no awareness of why it might not be such a good idea. What is needed is information about disclosure that could have adverse consequences. With that information, an informed judgment on the risks can be made. If there are risks in disclosure:

- is it in the public interest to provide access to the information?
- should it be provided only to those who can secure it?
- can the information be edited so it is less sensitive but still useful?

WHAT IS THIS GUIDE FOR?

This document describes the types of information which could be useful to terrorists and others of malign intent. It is intended as a guide, particularly to those unfamiliar with such matters, to the risks and dangers associated with automatic disclosure. It is intended to assist users in deciding whether information should be formally secured and whether to seek alternative means of achieving the same purpose.

WHAT THIS GUIDE IS NOT!

This is a *guidance* document. No obligations are implied by it and, importantly, it should not be regarded as contradicting any of the wide variety of legislation that requires certain types of information to be shared or made public. Its aim is to assist readers to be aware of, and where possible to minimise, the risks associated with those obligations.

PART 2

HOW TO USE THIS GUIDE

There should be a presumption of openness unless there are cogent and defensible reasons against it. The defensible reasons need to fit within the meaning of one of the exemptions in the Freedom of Information Act 2000. This Guide has been compiled in tabular form (Part 3) to inform decisions about which information, because of its potential value to terrorists, or others with malevolent intent, should not be disclosed. It should, for example, be of assistance to those compiling safety cases and planning applications. Such documents often contain sensitive information about a nuclear facility. This Guide may assist in identifying to the safety and local government authorities those parts of the documents which they should protect and not make available to the public.

This Guide is concerned with the sensitivity of information, including that held on computer systems, relating to nuclear material, ORM and facilities housing such material. The special objective of this Guide is to prevent the disclosure of information that could assist a person or group planning theft, blackmail, sabotage and other malevolent or illegal acts. Its application is an integral part of the protection of data on nuclear material, ORM and the facilities housing such material. These data fall into the following categories:

- information on the physical security arrangements in place to protect nuclear and other radioactive material and the facilities;
- technical guidance on security standards and requirements;
- information on the quantity and type of material at a facility and its location;
- inventories, throughput, output, storage capacity of facilities and accounting;
- detail of planned movements of nuclear or other radioactive material;
- technical information about the production or processing of nuclear materials;
- information contained in facility IT systems;
- information on computer systems important to security and to safety;

- information contained in safety cases;
- information contained in planning applications;
- information about the UKAEAC deployment and operations.

Official disclosure of information concerning nuclear materials, ORM and the facilities that contain such material should be considered only after this Guide has been consulted. The policy is not designed to protect commercial information, although it is recognised that, occasionally, some commercial information may contain sensitive material. Unless it conflicts with this Guide the release of such information would be at the discretion of local management.

Effective use of this Guide requires some understanding of the Protective Marking scheme used by government and the categorisation of nuclear materials.

- The *Protective Marking* scheme is a way of indicating that information should be seen only on a need-to-know basis and that it should receive appropriate protection. It is based on the damage that could arise if the information were to be seen outside of the need-to-know group. It is not usual to attach visible labels to physical assets but the same principles can be applied. The explanations used in this Guide for not releasing information are also those that would be used to determine the appropriate Protective Marking. It is convenient, therefore, to indicate the sensitivity of particular sorts of information through the use of the national system of protective markings as this is also indicative of the security levels that are required. The definitions of the national protective markings are given in Annex B.

- Nuclear materials, including nuclear waste depending on its nature, are placed into one of four *categories*, denoted by the characters I to IV. The importance of the material and, therefore, the protection applied to counter theft or sabotage is determined by the Category into which it falls. Material in Category I requires a greater level of protection that that in Category IV. Nuclear licensed sites are also given a similar category number dependent upon the material that is stored or processed there. The UK Categorisation Table is reproduced at Annex C.

PART 3

3.1 GUIDANCE TABLES

The tables in this Part provide detailed guidance to inform decisions about information that should not be released and the reasons why not. In some instances the reason for non-disclosure cites exemption given by sections of the Freedom of Information Act 2000 (a cross reference to the Freedom of Information (Scotland) Act 2002 is provided in Annex A). It should be understood that a malevolent act on a nuclear facility may give rise to a release of radioactivity which may be confined to the site or, worse, may affect an area surrounding the site. Information which, if disclosed, could lead to an action which could cause such a release of radioactivity would be exempt under section 38(1) of the FOI. Such information, depending on circumstances, could also be exempt under section 31(1)(g)and subsections (2)(i) and (j). These sections of the Act are implicit and, therefore not quoted in the tables. Also implicit are the provisions of Regulation 4(2)(a) of the Environmental Information Regulations which provides for exception of information, the disclosure of which would affect, inter-alia, public security.

Topic	Sensitivity	Reason for Protecting
0100 Security of Nuclear Material and Facilities		
0101 Regulations and Guidance		
a. Nuclear Industries Security Regulations (NISR) 2003	**Releasable**	**None**
b. Guidance to NISR 2003	**Not Releasable**	**This document contains procedures and operational details which would be of significant use to a person or group planning to attack a nuclear facility or transport**
c. Technical Guidance to NISR 2003	**Not Releasable**	**This document contains details of standards, types of equipment to be used, procedures and security operations details of which would be of great use to a person or group planning to attack a nuclear facility for the purposes of theft or sabotage. *(the information contained in the document has the protective marking (P-M) of* CONFIDENTIAL*)***
0102 Security Plans for Licensed Nuclear Sites		
All sites	**Not Releasable**	**Security plans contain detailed descriptions of the security regime in place at a site and**

Topic	Sensitivity	Reason for Protecting
		precise detail of where within the site nuclear material is stored and details of other areas vital to the site. Such information would be of great value to any person or group planning to attack a nuclear facility for the purpose of theft or sabotage. ***(Security plans for Category I to III sites would have a P-M of*** *CONFIDENTIAL.* ***Those for Category IV sites have a P-M of*** *RESTRICTED****)***
0103 Security Reports **a. Reports from security surveys, inspections and assessments and other reports on the physical security or technical security measures employed on a nuclear site.**	**Not Releasable**	Access to these reports can provide persons with malevolent intent with detail on the location of nuclear materials, the measures taken to protect them and any assessed vulnerabilities there may be; thus assisting them to avoid security measures and controls. ***(Security Reports will attract a P-M of at least*** *CONFIDENTIAL****)***
b. Reports describing critical features and/or highlighting requirements for security improvements for: • **Category I & II nuclear material** • **Category III nuclear material** • **Category IV nuclear material** • **Vital Areas**	**All below Not Releasable**	**Information of this nature will be of great assistance to persons wishing avoid security arrangements and assist with targeting a nuclear facility.** ***(These reports merit a P-M of*** *SECRET****)*** ***(These reports merit a P-M of*** *CONFIDENTIAL****)*** ***(These reports merit a P-M of*** *RESTRICTED****)***
c. Results of security investigations at a nuclear site, including those into leaks of sensitive information	**Not Releasable**	***(These reports merit a P-M of*** *CONFIDENTIAL****)*** **Exempt information under FOI, section 31(g) and subsections**

Topic	Sensitivity	Reason for Protecting
		(2)(b) or (i) or (j)
0104 Details of construction and layout of stores and process areas, including drawings or plans held on any media, showing features of physical security relevant to the prevention of theft or sabotage at: a. Category I & II b. Vital Areas and NPS c. Category III d. Category IV	**All Not Releasable**	**Official maps, chart or plans of sites may be released at the discretion of site management, provided they contain no description of the details of a building's functions, the materials stored therein and the location of internal security fences and the other security measures employed at the building.** **Knowledge of this nature can assist persons to avoid security arrangements and possibly assist with targeting.** ***(Information of this nature concerning Category I & II sites, Vital Areas and Nuclear Power Stations merits a P-M of*** *CONFIDENTIAL****; that for Category III & IV sites requires a marking of at least*** *RESTRICTED****)***
0105 The types and locations of intruder detection system (IDS) sensors and the associated CCTV cameras, including circuit diagrams and cable runs, and the maintenance and testing programmes for these equipments	**Not Releasable**	**Any details which could assist in the security systems at nuclear facilities being defeated by an attacker must be protected. FOI section 31(1)(a) may apply.** ***(This information merits a P-M of*** *CONFIDENTIAL* ***for Categories I and II and*** *RESTRICTED* ***for Categories III and IV)***
0106 Details of Automatic Access Control Systems (AACS), including the location of computer servers and back-up servers.	**Not Releasable**	**Any details that could lead to the AACS system being defeated by an attacker, insider or outsider, should not be released.** ***(Such information requires a P-M of*** *CONFIDENTIAL* ***for Categories I, II and Vital Areas and*** *RESTRICTED* ***for Categories III and IV)***
0107 Stores: security procedures for the issue, receipt and control of stock; names of authorised key holders; arrangements for monitoring and guarding:	**Not Releasable**	**Of great potential assistance to attackers (whether they be insiders or outsiders) who may be considering sabotage or theft of nuclear material.**

Topic	Sensitivity	Reason for Protecting
		(Information of this nature for Category I facilities attracts a P-M of up to *CONFIDENTIAL)*
0108 General maps showing the position and limits of a nuclear facility but without detail of what is contained therein	**Releasable**	**None** ***The Nuclear Installations Act 1965 requires the Minister to maintain a list of licensed sites and maps showing position and limits and to ensure the list is available to the public. This information does NOT attract a protective marking.***
0200 Information Relating to the Quantity and Form of Nuclear Material		
0201 Information about the quantity and form of nuclear material received or held in specified locations relating solely to civil nuclear programmes: **a. All Categories of site and NPS** **b. Exact locations where spent fuel is held** **c. List of spent fuel management facilities**	 **Not Releasable** **Not Releasable** **Releasable**	**Information of the sort contained in this section could be an aid to choosing targets while planning attacks.** ***(Information on sub-paras a and b normally attract a marking of*** *RESTRICTED**)*** **None**
0202 Throughput – nominal capacity, actual throughput and historical data on throughput of a plant under Safeguards	**Releasable**	**None**
0300 Nuclear Material in Transit (Including Movements within Sites)		
0301 Information on Category I - III movements	**Not Releasable**	**Information of this sort would be an aid to choosing targets while planning attacks for theft or sabotage on material in transit.** ***(information on Category I movements merits a marking of*** *CONFIDENTIAL* ***that of Category II and III movements a marking of*** *RESTRICTED**)***

Topic	Sensitivity	Reason for Protecting
0302 Information on Category IV movements	**Releasable with discretion**	**Information of this sort could be an aid in planning theft or sabotage attacks so information should be treated with care *(does NOT normally attract a protective marking***
0303 High Security Vehicles (HSV) **a. Visual access to interior of cab and cargo compartment** **b. Physical security features of vehicle design and construction** **c. Design and function of alarms, immobilisation devices and key designs for special locks** **d. Load compartment keys, spare keys and combination lock settings, where used**	 **Not Releasable** **Not Releasable** **Not Releasable** **Not Releasable**	**HSV carry fissile material and any information of the type listed in this section would be of use to an attacker planning an attempt to steal or sabotage fissile material in transit.** ***(The appropriate P-M for the various aspects opposite would be:*** ***a.*** *RESTRICTED* ***b and c.*** *CONFIDENTIAL* ***d.*** *SECRET**)***
0304 Vehicle tracking system; performance and communications	**Not Releasable**	**HSV carry fissile material and any information of the type listed in this section would be of use to an attacker planning an attempt steal or sabotage fissile material in transit.** ***(Detail of this nature would require a P-M of at least*** *RESTRICTED**)***
0305 Nuclear Material Transit Containers: **a. Level of resistance of transport containers of containers to attack by various means** **b. Specifications and design data on containers**	 **Not Releasable** **Releasable**	**Useful to an attacker planning a sabotage attack with the aim of releasing radioactive material, or theft of the material.** ***(This data is covered by the protective marking of*** *CONFIDENTIAL**)***
0400 IT Systems & Computer Systems Important to Security and Safety		

Topic	Sensitivity	Reason for Protecting
0401 Details of IT Systems storing and processing RESTRICTED information, the architecture of the systems and details of security measures employed and where back-up data is stored	**Not Releasable**	**Useful information for a person or group planning theft, sabotage or other malevolent act at a nuclear facility.** ***(Details of such systems would require a P-M of** RESTRICTED**)***
0402 Details of computer systems which perform access control for entry to and egress from a licensed nuclear site and to other facilities within the site and other security functions; and information on the location of back-up hardware and software	**Not Releasable**	**Information useful to a person or group planning theft, sabotage or other malevolent act at a nuclear facility.** ***(Detail of this nature would require a P-M of at least** RESTRICTED**)***
0403 Fact that systems controlling access may also have a safety mustering function	**Releasable**	
0404 Details of computer systems important to safety installed on licensed nuclear sites, including the locations, functions and upgrade routes for the systems and where back-up information is stored (SC = safety category): **a. SC 1 systems** **b. SC 2 & 3 systems**	**Not Releasable** **Not Releasable**	**Compromise of these systems could permit an attacker to at least disrupt the operations of a facility. In the worst case disruption could lead to a radioactive release.** ***(Details of such systems would require a P-M of** CONFIDENTIAL**)*** ***(Details of such systems would require a P-M of** RESTRICTED**)***
0500 United Kingdom Atomic Energy Authority Constabulary (UKAEAC)		
0501 The Constabulary **a. Overall establishment and the current strength of the force** **b. Establishment and current strength at particular sites** **c. Numbers on any shift at a site**	**Releasable** **Not Releasable** **Not Releasable**	**Available in CC's Annual Report** **Information of this nature would be very useful to any individual or group in planning an incursion into a nuclear site for the purpose of sabotage or theft and would seriously undermine the capability for effective response to an attack.** ***(Details of this nature would require a P-M of at least***

Topic	Sensitivity	Reason for Protecting
d. Number of authorised firearms officers at individual sites	**Not Releasable**	*RESTRICTED**)***
e. Armed response capabilities and timings at a site	**Not Releasable**	**Any information that would help a terrorist group to estimate in advance the scale of response and the capabilities available in a UKAEAC operational unit must be protected from disclosure.** ***(Details of such systems would require a P-M of** CONFIDENTIAL**)***
0502 UKAEAC escorts for movements:		
a. That escorting UKAEAC officers may be armed	**Releasable**	
b. Deployment and strength of escorts	**Not Releasable**	**Information of the nature contained in the last sub-paragraphs b and c would be of great use to an individual or group planning to attack a convoy** ***(Details of this nature would require a P-M of** RESTRICTED**)***
c. Radio frequencies in use to enable communication with County or Regional Police Forces	**Not Releasable**	
0600 Nuclear Material Accounting		
0601 Description		
a. Statements of general material accounting principles	**Releasable**	
b. Description and location of Material Balance Areas (MBA) and Key Measurement Points (KMP) not already in the public domain	**Not Releasable**	**Reveals details of location and quantities of fissile material that would be of use to an attacker planning theft of nuclear material or sabotage.**
c. Physical and chemical form of material measurement at KMP	**Not Releasable**	***(Details of this nature would attract a P-M of** RESTRICTED**)***
0602 Measurements and instrumentation data:		
a. Data which reveals the sensitivity of measurement or the alarm limits for MUF at a particular plant	**Not Releasable**	**Some precision and accuracy data relating to actual or typical measurements at sites, whether aggregated or disaggregated, could assist terrorists or others planning theft of material**

Topic	Sensitivity	Reason for Protecting
b. Precision and accuracy of standard laboratory techniques	**Releasable**	***(Details of this nature require a P-M of** RESTRICTED**)***
0603 Nuclear material flow and inventory data		
a. Nuclear material flow and inventory data held on IT systems, in hard copy or on any form of storage medium	**Not Releasable**	**Information of this nature could reveal exact details of the location and movements of nuclear materials** ***(Details of this nature would require a P-M of** RESTRICTED**)***
b. Inventory information in other records, if locations are referred to by code numbers and the key to the code is marked RESTRICTED	**Releasable**	
0604 Material Unaccounted For (MUF)		
a. Annual MUF figures for a site which do not reveal the MBA concerned	**Releasable**	**Following DTI's formal approval the companies in the civil nuclear industry publish annually an overall MUF figure for each of their sites for safeguarded plutonium, high enriched, low enriched, natural and depleted uranium. Provided that protectively marked or commercial information is not disclosed, questions arising from the publication of MUF figures can be answered. It is not intended that MUF data should be withheld solely on the grounds that it would cause embarrassment to the companies** ***(Details of this nature may attract a P-M of** RESTRICTED or higher**)***
b. MUF in MBAs or KMPs	**Not Releasable**	
d. Details of investigations into particular MUFs unless formally approved for release	**Not Releasable**	
e. Limit of Error for MUF (LEMUF) or other specific indications of the uncertainty of MUF figures	**Not Releasable**	
0700 Planning Applications		
0701 Planning applications should contain only the minimum information required by law:	**Releasable (with discretion)**	**If it becomes necessary to provide the planning authority with more than the basic**

Topic	Sensitivity	Reason for Protecting
a. Plans and drawings should contain only the detail necessary and must not indicate location of security equipment **b. Detailed description of the function of the building is to be avoided although building numbers may be used** **c. Fence lines may be indicated but detail of the fence structure should be avoided**		**information, this information should be contained in an annex and protectively marked appropriately. The planning authorities should be notified that is to be protected and is not for public consumption. Attention of the planners should be drawn to Section 79 of the Anti-Terrorism, Crime and Security Act 2001.** **Operators should consult the appropriate local authorities and apprise them of the sensitivity of any information in the application which requires protection and that it should not be available for public scrutiny** ***(some information that is attached to an application may attract a P-M of at least*** *RESTRICTED****)***
0800 Safety Cases and Other Safety or Environmental Information		
0801 Safety Cases **a. Safety cases of all classes** • **details of the potential hazards or other information that could be used as a surrogate for evaluating the impact of a release, or details on the impacts of releases;** • **details of strengths and weaknesses of processes, structures and protection systems designed to contain, control or secure material;** • **details of essential services which underpin systems and structures designed to contain, control or secure material;** • **details of access to the production process both**	**Not Releasable** **Not Releasable** **Not Releasable** **Not Releasable**	**The type of detailed information contained in safety cases would be of great use as an aid to a potential attacker for choosing targets and planning an operation.** ***(all of the information detailed in the bulleted list attracts a***

Topic	Sensitivity	Reason for Protecting
production process, both physical access control and the removal of material from the process for control and monitoring purposes. ***(note: any safety case which contains information included elsewhere in this Guide must take account of the sensitivity of that information)*** **b. Safety case summaries**	**Releasable**	***protective marking of at least*** *RESTRICTED****)*** ***For Safety Category (SC) 3 there may be no summary; the SC3 Log will substitute***
0900 Contingency and Emergency Plans & Exercises		
0901 Contingency and emergency plans **Existence of and details in Contingency and Emergency plans for a radiological incident at a facility**	**Releasable**	
0902 Security Contingency Plans **Detail in security contingency plans for a nuclear facility**	**Not Releasable**	**Such plans contain detailed information on the security regimes and procedures in place. They would also contain information on the capabilities of the police or guard force contingents and on the likely response to a security incident. All would be very useful to a would-be attacker. FOI section 31(1)(a) may apply.** ***(Details of this nature would require a P-M of at least*** *RESTRICTED****)***
0903 Exercises **a. That an exercise is to take, or has taken place**	**Releasable**	

Topic	Sensitivity	Reason for Protecting
b. Details of security exercises at a facility	**Not Releasable**	**Provides would-be attackers with information concerning nature and timing of response, detail of armed response force, nature of tactics employed and signal plan *(Depending on the nature of the exercise, a P-M of* RESTRICTED *or* CONFIDENTIAL *may apply)***
c. Details of safety exercises	**Releasable (with discretion)**	**Information concerning the location and contents of buildings at a facility of particular sensitivity should not, however, be released, as it would provide a potential attacker with useful planning information**
1000 Personal Information		
1001 Personal information		**Information of this nature could be used by a potential attacker to attempt to suborn or otherwise exert pressure on an individual working at a facility or on an individual associated with a facility. *(Protection for this type of information is afforded by vetting confidentiality and by the Data Protection Act. It would normally be covered by the P-M of* RESTRICTED - STAFF*) See also s40 of FOI***
a. Information in vetting files	**Not Releasable**	
b. Information in personal files	**Not Releasable**	
1100 Radioactive Waste Inventory		
1101 Information on radioactive waste streams:		
a. General information that does not identify a building or location and does not contain any other information that would be exploitable	**Releasable**	
b. Information that enables a specific building at a facility and the material	**Not Releasable**	**Provides targeting information for an attacker planning sabotage**

Topic	Sensitivity	Reason for Protecting
held there to be identified		***(Details of this nature would require a P-M of** RESTRICTED**)***
1102 The BRIMS database, which contains very detailed Radwaste information supplied by operators. **(*Note: some specific information is extracted from the database to prepare Defra's national inventory of waste*)**	**Not Releasable**	***(Details of this nature would require a P-M of** RESTRICTED**)***
1200 Decommissioning		
1201 Plans to decommission plant, provided detail of precise quantities and locations of nuclear material or waste are not revealed	**Releasable**	
1202 Waste from decommissioning **a. That a store is to be built and location** **b. Detail of the construction, security measures and quantity of material to be stored in new builds for the treatment and storage of waste and arisings** **c. Details in contracts concerning security of waste streams, routes, storage** **d. Details of quantity, type and location of waste and arisings stored**	**Releasable** **Not Releasable** **Not Releasable** **Not Releasable**	**Provides good targeting information for an attacker planning sabotage attacks.** ***(Details of this nature would require a P-M of** RESTRICTED**)*** **Would provide advance targeting information to a person or group intending to attack a facility.** **(*could attract a P-M of up to** CONFIDENTIAL**)**
1300 Historical Information		
1301 Historical information, not already in the public domain, that contains information currently relevant and still sensitive (in relation to the other sections in this document), whether or not a protective marking has been applied.	**Not Releasable**	**Information of this nature, although old, may still be of use to malevolent persons planning action against a facility.** ***(Could be protectively marked up to and including** SECRET**)*** ***Operators should review their***

Topic	Sensitivity	Reason for Protecting
		historical data to ascertain what might fall into this category
1400 Threat Assessments and Security Alerting Information		
1401 Annual threat assessments issued by DCNS	**Not Releasable**	**Exempt under FOI section 23(1)** ***(Protectively marked up to and including** SECRET**)***
1402 Design Basis Threat	**Not Releasable**	**Exempt under FOI section23(1)** ***(Protectively marked up to and including** SECRET**)***
1403 Reasons for Alert State in place and for changes in Alert States	**Not Releasable**	**Exempt under FOI section 23(1)** ***(Protectively marked up to and including** SECRET**)***

Annex A

LEGISLATION ON DISCLOSURE

The access provisions of the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 come into force on 1 January 2005 and create a statutory right of access to information held by a Public Authority and provide a scheme for making information available. The Acts cover a wide range of public authorities and include public companies (see section 6 and Schedule 1); included are central government, local government, NHS bodies, schools, colleges, the police; other public bodies and offices. UKAEA is a public authority under Schedule 1 Part VI and BNFL another, under section 6 of both the FOI Acts. Section 6 does not appear to apply to other companies in the civil nuclear industry, although each should review its position thereunder. Section 4(1) of both Acts, however, provides that the Secretary of State (or Scottish Minister) may, if certain conditions are met, add to the schedule. On its formation, the Nuclear Decommissioning Authority (NDA) is likely to be one such addition.

Regulated by a Commissioner to whom the public have direct access, the FOI Act permits people to apply for access to information only. Whilst providing such right of access, the Acts also create exemptions from the duty to disclose and establishes the arrangements for enforcement and appeal. The Act also requires public authorities to inform the individual who requested it the basis for refusing a request for information, which must be made on the basis of the exemptions in the Acts.

Information may be withheld legitimately under the FOI Acts where an exemption applies or a public interest test is satisfied. Simply because information attracts a protective marking does not mean that it cannot be disclosed. In reality, however, if information has been protectively marked appropriately it is highly likely that the 'public interest' considerations that the Acts require have been taken into account and that the information may be withheld.

Environmental legislation provides for the placing of information relating to activities under various regulatory regimes on public registers. In most cases the Secretary of State has the power to direct that information should be withheld on the grounds of national security. In addition, the Environmental Information Regulations 1992 (as amended) require the provision of "environmental information" by certain public bodies upon request. This requirement is subject to certain exceptions, notably where disclosure would affect international relations, national defence or public security. Further amendments to the 1992 Regulations are likely to be made shortly.

FREEDOM OF INFORMATION ACTS

Part 2 of both the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 detail information that is exempt from disclosure, without being subject to a public interest test. The relevant Sections in each Act are, however, not always the same. When in this document there is a reference to a Section of the Freedom of Information Act the reference is from the FOI Act 2000. The comparison table and notes below enable cross-reference between the two Acts.

Aspect	FOI Act 2000 Section No	Scottish Act 2002 Section No
National Security	24	Both 31
Defence	26	
International Relations	27	32
Economy	29	Both 33
Commercial interests	43	
Public authority investigations	30	34
Law enforcement	31	35
Effective conduct of public affairs	36	30
Health and Safety	38	Both 39
Environmental	39	
Personal information	40	38
Information provided in confidence	42	36
Disclosure of environmental information	74	62
Removing restrictions on disclosure	75	64

General Points

Where the FOI Act 2000 defines exempt information as that which "would, or would be likely to, prejudice", the Scottish Act states "prejudice substantially".

The FOI Act 2000 has "The duty to confirm or deny does not arise if, or extent to which compliance with section …..". The Scottish Act does not have this provision.

In the Scottish Act "Scottish Ministers" replaces the "Secretary of State" throughout.

National Security and Defence

Whereas the FOI Act 2000 requires a Minister of the Crown to certify information is exempt, the Scottish Act requires a Member of the Scottish Executive to do so.

Public Authority Investigations/Law Enforcement

The differences between these sections in the FOI Act 2000 and in the Scottish Act are to take account of Scottish law and associated terminology.

Effective Conduct of Public Affairs

The FOI Act 2000 has the requirement for judgements to be made "in the reasonable opinion of a qualified person", the Scottish Act does not contain this provision.

Information Provided in Confidence

S36(1) of the Scottish Act – Information in respect of which a claim to confidentiality of communications could be maintained in legal proceedings is exempt information – this is not reflected in S41 of the FOI Act 2000.

Annex B

DEFINITIONS OF PROTECTIVE MARKINGS

SECRET (S) **The compromise of SECRET information or material would be likely:**

- **to raise international tension; to damage seriously relations with friendly governments;**
- **to threaten life directly, or seriously prejudice public order, or individual security or liberty;**
- **to cause serious damage to the operational effectiveness or security of the UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations;**
- **to cause substantial material damage to national finances or economic and commercial interests**.
- *to be of exceptional use to an individual or group planning a malevolent act against a nuclear facility or material transport*

CONFIDENTIAL (C) **The compromise of CONFIDENTIAL information or material would be likely:**

- **to materially damage diplomatic relations (ie cause formal protest or other sanctions);**
- **to prejudice individual security or liberty;**
- **to cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations;**
- **to work substantially against national finances or economic and commercial interests;**
- **substantially to undermine the financial viability or major organisations;**
- **to impede the investigation or facilitate the commission of serious crime;**
- **to impede seriously the development or operation of a major government policies;**
- **to shut down or otherwise substantially disrupt significant national operations.**
- *to be of substantial use to an individual or group planning a malevolent act against a nuclear facility or material transport*

RESTRICTED (R) The compromise of RESTRICTED information or material would be likely:

- **to affect diplomatic relations adversely;**
- **to cause substantial distress to individuals;**
- **to make it more difficult to maintain the operational effectiveness or security of UK or allied forces;**
- **to cause financial loss or loss of earnings potential to or facilitate improper gain or advantage for individuals or companies;**
- **to prejudice the investigation of crime;**
- **to facilitate the commission of crime;**
- **to breach proper undertakings to maintain the confidence of information provided by third parties;**
- **to impede the effective development or operation of government policies;**
- **to breach statutory restrictions on disclosure of information;**
- **to disadvantage government in commercial or policy negotiations with others;**
- **to undermine the proper management of the public sector and its operations.**
- *to be of significant use to an individual or group planning a malevolent act against a nuclear facility or material transport*

Annex C

CATEGORIES OF NUCLEAR MATERIAL

MATERIAL	CATEGORIES	
	I/II	III
1. Plutonium (other than plutonium with an isotopic concentration exceeding 80% in plutonium-238) which is not irradiated	More than 500 grammes	500 grammes or less, but more than 15 grammes
2. Uranium-233 which is not irradiated	More than 500 grammes	500 grammes or less, but more than 15 grammes
3. Previously separated Neptunium-237 which is not irradiated	More than 1 kilogramme	1 kilogramme or less, but more than 15 grammes
4. Previously separated americium-241, previously separated americium-242m or previously separated americium-243, which are not irradiated	More than 1 kilogramme	1 kilogramme or less, but more than 15 grammes
5. Uranium-235 in enriched uranium containing 20% or more of uranium-235, which is not irradiated	More than 1 kilogramme	1 kilogramme or less, but more than 15 grammes
6. Uranium-235 in enriched uranium containing 10% or more, but less than 20% of uranium-235, which is not irradiated	10 kilogrammes or more	Less than 10 kilogrammes, but more than 1 kilogramme
7. Uranium-235 in enriched uranium containing less than 10% but more than 0.711% of uranium-235, which is not irradiated		10 kilogrammes or more
8. Irradiated reactor fuel being used, stored or transported within the United Kingdom		Any quantity
9. Irradiated reactor fuel being transported outside the United Kingdom, other than such fuel which, prior to being irradiated, was uranium enriched so as to contain 10% or more, but less than 20% of uranium-235	Any quantity	
10. Irradiated reactor fuel being transported outside the United Kingdom which, prior to being irradiated, was uranium enriched so as to contain 10% or more, but less than 20% of uranium-235		Any quantity
11. Other irradiated nuclear material		Any quantity

Annex D

GLOSSARY

The following abbreviations are used within this document:

AACS	**Automatic access control system**
ATC&S	**Anti-terrorism, Crime and Security Act 2001**
BE	**British Energy**
BEGL	**British Energy Generation Ltd**
BEG(UK)L	**British Energy Generation (UK) Ltd**
BNFL	**British Nuclear Fuels**
BRIMS	**British Radwaste information Management System**
CCTV	**Closed circuit television**
DCNS	**Director of Civil Nuclear Security**
FOI	**Freedom Of Information Act 2000**
FOI(S)	**Freedom of Information (Scotland) Act 2002**
HSV	**High Security Vehicles**
IAEA	**International Atomic Energy Agency**
IDS	**Intruder detection system**
KMP	**Key Measurement Points**
LEMUF	**Limit of Error for MUF**
LMU	**Liabilities Management Unit**
MBA	**Material Balance Area**
MOD	**Ministry of Defence**
MUF	**Material Unaccounted For**
NDA	**Nuclear Decommissioning Authority**
NPS	**Nuclear power stations**
OCNS	**Office for Civil Nuclear Security**
ORM	**Other Radioactive Material**
PIDS	**Perimeter intruder detection system**
P-M	**Protective Marking**
SC	**Safety Category**
UCL	**Urenco (Capenhurst) Ltd**
UKAEA	**United Kingdom Atomic Energy Authority**
UKAEAC	**United Kingdom Atomic Energy Authority Constabulary**

Appendix 3

Selection Criteria for Working Groups

SELECTION CRITERIA FOR WORKING GROUPS

One output from Main Group meetings of stakeholders in the BNFL National Stakeholder Dialogue will be the formation of Working Groups. These Working Groups will carry forward more detailed elements of the work and report back to the next Main Group meeting.

Experience of Working Group meetings demonstrates that around 15 members provides a cohesive, practical and effective group. If there are more volunteers than places, a number of criteria will inform the Co-ordinating Group's selection from the volunteers.

People participating in the Working Groups must:

- represent a particular constituency and/or have relevant experience or expertise relevant to the Working Group;
- have been inducted into the process and style of working;
- accept and conform to the ground rules, and participate in their review and development;
- develop, observe and work in a co-operative spirit in the Working Group, while respecting that profound differences of opinion may exist;
- be a competent and collaborative negotiator (rather than a positional/competitive bargainer);
- be available for the full series of Working Group meetings (which may be 1 to 1½ days
  every month or 6 weeks) and Main Group meetings;
- be willing to undertake work between meetings, signposting or providing papers and reviewing information within the timescales agreed within the Working Group (this may be up to 1 week's work per month).

In addition to the above, the overall group profile will also influence Co-ordinating Group's choice. Ideally, each working group will need to contain representatives from the following sectors

- communities;
- company;
- customers;
- environmental NGOs;
- other NGOs;
- government;
- regulators;
- workforce;

and will need to be balanced in terms of the necessary skills.