Industry comments on RD /GD-338 Security Measures for Sealed Sources

Document section/excerpt of section	Industry issue	Suggested change
General Comment – The term Category 1, 2, 3, 4 and 5 as it relates to sealed sources is easily confused with Category I, II, III nuclear material as defined in schedule 1 of the Nuclear Security Regulations.		Bruce Power recommends using the "security group" terminology outlined in IAEA-TECDOC-1355 Table 2 (e.g. Security Group A, B, C, D) to eliminate confusion.
General Comment – This Regulatory Document is intended to govern security for sealed sources used in a variety of facilities, industries and environments. High security sites already comply with the *Nuclear Security Regulations* and related standards to protect Category I, II, III nuclear material against theft or sabotage. This includes access controls, physical barriers, intrusion detection systems, personnel and vehicle search, security clearance and an on-site armed nuclear response force capable of defending against the Design Basis Threat and any other credible threat identified by a threat risk assessment. Bruce Power requests confirmation from the CNSC that requirements in this RD related to access controls, detection of unauthorized access, physical barriers and intrusion detection systems are covered by existing measures implemented by licensees at high-security sites.		As an alternative, the CNSC could consider making this RD applicable to non high-security sites only and create a guidance document specific to high-security sites taking into account security measures already required by the NSRs. This would eliminate confusion and the need for interpretation. Confirmation on interpretation requested.
General Comment - The format of RD-338 is confusing in that it moves between "requirements" and "guidance".		Bruce Power recommends RD-338 be formatted similar to other regulatory documents which better streamlined and read more easily.

Document section/excerpt of section	Industry issue	Suggested change
Table B: Security levels and security objectives	Table B provides a good format in that it outlines requirements specific to each source category; it is easy to read and understand. The table, however, is inconsistent with the body of the RD.	Bruce Power recommends the RD be updated to align the table contents with the RD contents once the details have been fully vetted and revised through the review/comment process.
3.1.2 Guidance for general security measures The licensee should develop and maintain a threat and risk assessment to determine vulnerabilities in the existing physical protection systems designed to protect against the loss, sabotage, illegal use, illegal possession, or illegal removal during the storage or transportation of the sealed source. The threat and risk assessment, updated annually, is also used to determine mitigating security measures to address identified threats, manage risks or reduce/eliminate vulnerabilities.	The threat risk assessment should be reviewed annually and updated only as required based on changes that impact the threat level.	Bruce Power recommends submissions to the CNSC are required only when changes are made to the threat risk assessment. Bruce Power supports an annual review of the TRA.
3.2 Technical security measures **3.2.1 Requirements for technical security measures** Technical security measures for radioactive sources, devices or facilities shall include physical measures to: - prevent unauthorized personnel from gaining access to such sources - protect against an act or attempted act of unauthorized removal	The IAEA document specifies which technical security measure is required for the category classification. This document should also specify how these requirements apply to the different categories as some expectations differ from the IAEA document. It implies that the same rigor for technical security measures is applied to all categories.	Bruce Power recommends the technical measures be revised to more clearly align with the category type in accordance with IAEA guidelines.

Document section/excerpt of section	Industry issue	Suggested change
- protect against an act or attempted act of sabotage Technical security measures **shall also** include hardware and/or security systems designed according to the principle of defense in depth and the physical protection system functions of **"detection, delay and response".** This section includes security requirements for the following measures: - access control - **detection of unauthorized access** - locking hardware and key control - physical barriers (secure containers, secure enclosures) - **alarm response protocols** - **inspection, maintenance and testing of physical security-related equipment** - security officers In support of paragraphs 3(1)(*g*) and 3(1)(*h*) of the *General Nuclear Safety and Control Regulations*, the licensee **shall** include in their licence application details pertaining to physical security measures for access control, physical barriers, detection of unauthorized access, maintenance and testing of physical security-related equipment.		
3.2.2.2 Guidance for access control To control access to the sealed sources, the licensee should: • prevent unauthorized access to the sources • monitor and maintain records of all personnel with access to secure storage areas, through the use of a log book or an access control system with tracking capabilities • implement effective access control measures, such as manually activated locking devices,	Bullet 3 provides a variety of options for implementing access control measures that range from rudimentary to highly robust. Bullet 4 states that the system should incorporate measures to prevent "pass back" or "tailgating". This is not aligned with the simple measures identified in bullet 3 (e.g. a manually activated locking	Bruce Power recommends the body of the RD provide clarity regarding requirements for each specific category of sealed source to eliminate the need for interpretation.

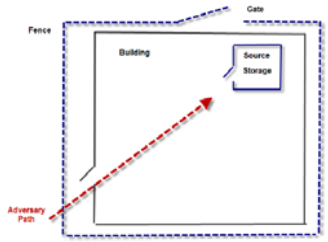
Document section/excerpt of section	Industry issue	Suggested change
padlocks, card reader access and biometric devices/systems, and through the use of "controlled" entry points • ensure the access control system incorporates measures to prevent unacceptable practices such as "pass back" or "tailgating" • assign individual personal identification number (PIN) codes if used in conjunction with an access control system • remove access rights for individuals as soon as access is no longer required • restrict access rights to the access control management system and software, to prevent unauthorized interference with the system database (hacking, software sabotage) • implement a means of duress signaling near the source storage, to provide notice to the alarm monitoring company or response personnel • implement a local alarm that triggers in the vicinity of the storage area, to alert nearby personnel of an intrusion or other problem in the source storage area	device or padlock would not prevent pass back or tailgating). It seems the intent of this section is to provide options based on the category of sealed source in the storage area to enable a graded approach to implementation of security measures. Bruce Power requests confirmation that systems currently installed at high-security sites to detect unauthorized removal of nuclear material on exit meet the intent of the requirements pertaining to alarming at the storage area. Bruce Power requests confirmation that robust security measures required at high-security sites negates the need for duress signalling to the monitoring room. Bruce Power believes this measure is intended for facilities/environments that don't have a complex security program already in place.	See also comments for Table B. Confirmation on interpretation requested. Bruce Power is requesting clarification on the following bullets: Bullet 5: What is the rationale for requiring a PIN code for entrance into a source storage room - Are requirements only imposed if an electronic access control system is utilized? Bullets 8-11: If a manual access control system is used (ex. pad lock, door lock, cabinet lock) then is an alarming system required?
3.2.2.2 Guidance for access control The security program should include security measures relating to detection, delay and response to security events (e.g., alarm detection devices, fencing, secured storage containers, immobilization of vehicles and/or trailers, security officers).	This statement is out of place. Section 3.2.2.2 is specific to technical measures for access control and this statement refers to the overall security program	Bruce Power suggests this statement be removed.
3.2.3.1 Requirements for detection of unauthorized access	This section provides a range of options	Bruce Power recommends the

Document section/excerpt of section	Industry issue	Suggested change
The licensee shall implement measures for the detection of attempted or actual unauthorized access in a timely manner, such as: • visual observation • video alarm assessment • detection devices • accountancy records, seals, or other tamper-indicating devices including process monitoring systems (for example, daily or twice-weekly audits, to ensure that the sources are present) Note that, for mobile sources in use, continuous visual surveillance by operator personnel equipped with an appropriate communication link may substitute for one or both layers of barriers. If an intrusion detection system is used, it must: • immediately detect any unauthorized intrusion into the sealed source storage area • immediately detect any tampering that may cause any of the alarm system devices to malfunction or cease to function • when an intrusion is detected, set off a continuous alarm signal that is both audible and visible at the licensee's location and/or at an approved monitoring station, using a supervised communications link; the monitoring station shall be certified by a body accredited by the Standards Council of Canada, or other certification body deemed acceptable by the CNSC staff • include an uninterruptible power supply subject to routine testing, to ensure continuous operability of the security detection system	from basic (daily or twice-weekly audits) to robust (detection devices, video alarm assessment). This is the same issue identified for section 3.2.2.2. It seems these options are intended to allow for graded security measures commensurate with the category of source (or threat/risk level). Bruce Power recommends the requirements to be "equipped with an appropriate communication link" not apply to operators using a mobile source inside a high-security site protected area. Section 3.2.3.1 provides a variety of options for detection of unauthorized access, including records, seals, daily or twice-weekly audits. It then states "IF" an intrusion detection system is used, it must do certain things. This leads the reader to believe there are options and an alarm system is but one of them	body of the RD provide clarity regarding requirements for each specific category of sealed source to eliminate the need for interpretation. Bruce Power suggests this section identify an exemption for high-security sites. See comment at section 3.2.3.2

Document section/excerpt of section	Industry issue	Suggested change
3.2.3.2 Guidance for detection of unauthorized access To detect unauthorized access, the alarm system should: • activate immediately upon detecting an intrusion or tamper event • stay in an alarmed state until acknowledged by an authorized person • have two or more zones for each area of storage • have an acceptably low nuisance and/or false alarm rate • be certified by the Underwriters Laboratories (UL) or Underwriters Laboratories of Canada (ULC) The licensee should: • ensure that alarm monitoring devices and back-up battery power are protected against tampering by unauthorized personnel (e.g., electronic panel or junction box) • ensure the keypad is installed within a secure environment, to prevent tampering • use dedicated alarm zones in the storage area (separate from any other alarm zones) and limit access to authorized users only • maintain an audit trail to record the cause of any alarms	Further from comment related to section 3.2.3.1. This section provides "guidance" to further describe how the section above can be implemented. This guidance only provides input on an alarm system which leads the reader to believe that an alarm system is the only option as it does not provide guidance on any other option.	Bruce Power requests guidance pertaining to the other options for detection of unauthorized access as described in section 3.2.3.1. NOTE: this issue is similar to other issues raised regarding describing the graded approach to security.
3.2.5.1 Requirements for physical barriers For sealed sources whose activity is less than the threshold levels listed for Category 3 in Table A, the licensee shall store the sources in secure containers, as described in section 3.2.5.1.1. For sealed sources whose activity is equal to or above the threshold levels listed for Categories 1, 2, or 3 in Table A, the licensee shall implement a minimum of two different physical barriers, to prevent unauthorized access to sealed	Bruce Power requires clarification on Paragraph 2. This requirement seems excessive and is not consistent with the IAEA "Security of Radioactive Sources" document requirements. Although Bruce Power meets these requirements, the IAEA suggests that only Category 1 storage areas have two technical ("physical") barriers and Category 3&4 only require one technical	Bruce Power requests clarification. Bruce Power suggests this section identify an exemption for high-security sites.

Document section/excerpt of section	Industry issue	Suggested change
sources in storage or provide delay sufficient to enable response personnel to intervene as required. The physical barriers shall be any combination of secure containers or other secure enclosures. For example: • a licensee who stores a sealed source in a locked safe may locate the safe in an enclosed room that can be locked, and must secure the container in place (floor, wall or vehicle) • alternatively, the safe may be located within a locked metal cage or other suitable enclosure • the access-controlled perimeter of the licensee's location may serve as the first secure enclosure, with a secondary secure enclosure or secure container inside, both with access Control Note that for a mobile source in use, it may not always be possible to achieve the security measures specified above. In such cases, compensatory measures shall be implemented to provide other forms of protection (e.g., close supervision combined with an appropriate communication link).	barrier. Bruce Power recommends the requirements to be "equipped with an appropriate communication link" not apply to operators using a mobile source inside a high-security site protected area.	
3.2.5.1.2 Requirements for secure enclosures Enclosures include rooms, buildings or cages that can be secured. For an enclosure to be considered secure, all exterior components (e.g., walls, doors and windows) are resistant to physical attack using handheld tools and access/egress points are equipped with access control devices, or access is controlled by security officers. Windows that provide access to interior areas in proximity to	Bruce Power requires clarification. Does this requirement apply to all category sources or to just Category 1, 2, 3? This requirement seems excessive for Category 3 sources and below. Bruce Power requires clarification on the door material requirement. This requirement is excessive for licensed storage/use locations that are located	Bruce Power requests clarification.

Document section/excerpt of section	Industry issue	Suggested change
sources must be equipped with bars (where the gap between the bars must be less than 15 cm), metal grill, expanded metal mesh, and/or retrofitted with a UL/ULC certified security film or glazing. Security hardware attached to windows must be affixed from the inside to prevent tampering, or fitted with tamper-resistant devices if fitted from the outside. Doors that provide access to areas where nuclear substances and radiation devices are used, processed or stored must be secured when left unattended. Doors must be solid-core wood or metal clad and installed in a reinforced frame of equivalent material. Doors must be maintained in good state of repair and fitted with non-removable pinned hinges, if the hinges are mounted on the outside. Any door glazing or large vents (grills) must be fitted with security glazing or bars, metal grills, or equivalent. Grills must be secured in place with tamper-resistant devices.	within nuclear generating stations as PROL security requirements apply. How does this requirement apply to licensees that have to comply with the Class I Nuclear Facilities and Nuclear Security requirements?	
3.2.5.2 Guidance for physical barriers Traditional barriers such as chain-link fences, locked doors, grilled windows, masonry walls and vaults are commonly used for storage of radioactive sealed sources. Barriers should be considered in relation to an adversary's objectives. The licensee should implement multiple physical barriers to protect the radioactive sources. Multiple barriers potentially force an adversary to bring a variety of tools to defeat each	Bruce Power requires clarification on this section of the document. Are multiple barriers required for all category of sources or only Category 1, 2, 3? If it excludes lower category sources, then the document should state that.	Bruce Power recommends the body of the RD provide clarity regarding requirements for each specific category of sealed source to eliminate the need for interpretation.

Document section/excerpt of section	Industry issue	Suggested change
individual barrier, thereby delaying the adversary and providing the response personnel with time to intervene. One implementation of the concept of defense in depth is to have multiple layers of different barrier types along the path to complicate an adversary's progress by requiring a variety of tools and skills (see Figure 1).  Figure 1: Adversary path to a storage area For example, multiple barriers may include: - a portable device (e.g., portable gauge, exposure device) stored inside a vault or safe that is bolted to the floor and capable of resisting common attack tools - a mobile device (e.g., a brachytherapy unit) may be chained to the floor within the storage area. The chain is made of material resistant to common attack tools and is secured with a good quality padlock that has the same level of robustness (e.g., shielded shackles) - a solid-core door made of wood or metal, installed with non-removable screws, pinned door hinges, a latch protector and an automatic door closer a window equipped with laminated window-film resistant to burglar attacks, metal mesh or metal bars spaced at 15 centimetres or less, and installed with non-removable screws		
3.2.5.2.1 Guidance for secure containers	Bruce Power requests confirmation that	Confirmation on interpretation

Document section/excerpt of section	Industry issue	Suggested change
The storage location and/or container should: • be secured with a locking mechanism or have other measures to prevent unauthorized removal • be secured when left unattended • be equipped with an alarm system to detect unauthorized entry or access • be sufficiently robust to resist common attack tools (e.g., sledgehammer, crowbar, drill, blowtorch)	security requirements for protected area perimeter at high-security sites meets the intent of an alarm system to detect unauthorized entry or access.	requested.
3.2.5.2.2 Guidance for secure enclosures Openings, such as windows or vent ducts, that could provide access to secure enclosures should be fitted with bars, a metal grill, expanded metal mesh, and/or retrofitted with a UL/ULC certified security film or glazing. Security hardware attached to windows should be affixed from the inside, to prevent tampering, or be fitted with tamper-resistant anchors if affixed from the outside. Doors that provide access to areas where radioactive sealed sources and/or radiation devices are used, processed or stored should be secured when unattended. The material used for the door should be solid-core wood or metal-clad, and the door should be installed in a reinforced frame of non-secure side, the door should be fitted with non-removable pinned hinges. Any door glazing or large vents (grills) should be fitted with security glazing or bars, a metal grill, or equivalent. Grills should be secured in place with tamper-resistant anchors.	Bruce Power requires clarification on this section of the document: Section 3.2.5.2.2. Is there an international guidance document that can be referenced instead of placing the requirements into this document?	Bruce Power recommends the RD reference an international standard rather than describe detailed requirements.

Document section/excerpt of section	Industry issue	Suggested change
If continuous visual surveillance is done by an operator, the operator should be equipped with a means of communication (e.g., cell phone or radio) and should be aware of the response protocols to communicate rapidly to response personnel in the event of unauthorized access or removal. If key pads are used to arm and disarm an intrusion detection system, the device and its electric junction box should be installed in a secure area, to reduce the risk of tampering. To maintain continuous power to the alarm monitoring detection system in the event of a loss of primary power, the licensee should consider implementing an alternate or auxiliary power back-up source, or equivalent, to maintain detection capability.		
3.3.2.1 Requirements for a site security plan For Category 1, 2 and 3 sources, technical and administrative measures shall be documented by the licensee in a site security plan, appropriately designated in accordance with section 12(1)(*j*) and 21 to 23 of the *General Nuclear Safety and Control Regulations*. The site security plan shall be updated and verified by the licensee at least once a year, to address any changes within the licensed facility.	The site security plan should be reviewed annually and updated only as required based on changes to the physical or operational security measures.	Bruce Power recommends submissions to the CNSC are only required when changes are made to the site security plan.
3.2.6 Alarm response protocol **3.2.6.1 Requirements for alarm response protocol** The licensee **shall** respond immediately to any actual or attempted theft, diversion or sabotage to radioactive	Bruce Power requires clarification on this section. Section 3.2.3.1 implies that an alarm detection system is an option among the list that is provided as examples. This section insinuates that an alarm is required and a response plan for that alarm is	Bruce Power recommends the RD be revised to be more clear regarding what is required.

Document section/excerpt of section	Industry issue	Suggested change
material or devices. The licensee **shall** develop and maintain a documented alarm response protocol to record the cause and dispensation of alarms. The protocol **shall** include the role and responsibilities of the licensee's emergency response staff and offsite response force, and **shall** be documented in a contingency plan or an equivalent document. The licensee must notify the local police force of jurisdiction, informing them that sealed sources are onsite, and include an opportunity for onsite familiarization tours. The licensee **shall** develop and maintain written arrangements with offsite emergency responders, and update those arrangements annually or when changes to the facility design or operations affect the potential vulnerability of the source. Written arrangements are not required for temporary job sites.	mandatory.	
4. Security Measures for Sealed Sources during Transport **4.1 Vehicle security** **4.1.1 Requirements for vehicle security** For the transport of a Category 1 source, the vehicle **shall** be equipped with: - a vehicle tracking device that enables the vehicle to be recovered if stolen - a duress alarm or an equivalent device that is continuously monitored; the licensee **shall** instruct the alarm monitoring station to alert the appropriate response force (e.g., police agency of jurisdiction) -	Bruce Power requests clarification on Section 4. Are there any requirements for sources that are shipped by other means of transport (via air, sea, rail, etc)?	Bruce Power recommends the RD be updated to include requirements for all modes of transport.

Document section/excerpt of section	Industry issue	Suggested change
For Category 1, 2 and 3 sources, the licensee's vehicles **shall** be equipped with anti-theft devices. **The anti-theft devices shall consist of:** - **a vehicle disabling device (e.g., starter disabler that prevents the start of the vehicle without a proper key or a similar start device)** - **if the vehicle is left unattended, a device that immediately detects unauthorized entry or attack to the vehicle and triggers an audible or visible alarm. If the vehicle operator is not within hearing or visual range of the alarm, the operator shall have the ability to monitor the alarm devices remotely** These anti-theft devices **shall** be activated automatically or manually by the operator at any time when the vehicle containing the package is left unattended. While being stored during transportation, the package **shall** either be stored in a secure container in the vehicle, or in a location that is protected by physical security measures and is continuously monitored when the package is left unattended. For Category 4 and 5 sources, the licensee **shall** implement prudent management practices by using effective access control and ensuring the security of radioactive material and devices at all times.		
4.2 Security measures for sealed sources during transport **4.2.1 Requirements for security measures for sealed**	Is the shipping document describing the security measures for sealed source in addition to the current shipping document	Bruce Power recommends Para. 2 be reworded to align with the wording in the P&TNSR

Document section/excerpt of section	Industry issue	Suggested change
sources during transport As the licensee (the consignor) is responsible for the safety and security of sealed sources during transport, the licensee **shall** ensure the authorized carrier is capable of providing physical security measures for sealed sources while they are in transport or being stored during transportation. As required by the *Packaging and Transport of Nuclear Substances Regulations*, the licensee **shall** provide the carrier with the appropriate shipping documents relating to the sealed source. The shipping documents **shall** include the corresponding description of security measures for sealed sources. Where more than one category of radionuclide applies (e.g., for shipments of multiple radionuclides) the applicable measures **shall** be based on the more restrictive category. All packages containing sealed sources of Category 1, 2 or 3 **shall** be protected from unauthorized access, theft or unauthorized removal during transport and temporary storage during transport. The consignee should be notified when, where and by whom such packages are being moved, including tracking numbers and expected arrival times. The licensee, being the consignor, **shall** contract a carrier with a proven record for the safety and security of dangerous goods while in transport, and **shall** take the following precautions:	required ? Please clarify "more than one radionuclide" does this mean a single sealed source containing multiple nuclides, or if there are multiple radionuclide per consignment (i.e. multiple packages in one shipment?) This section is vague as to what the paperwork should specify. It must be more detailed and should be cross-referenced in the Packaging and Transport of Nuclear Substances Regulations. Perhaps there should be a section for "Transport documents" if security measures document is mandatory. Section 4.2.1: "the consignor, shall contract a carrier with a proven record for the safety and security of dangerous goods". If the shipment is not exclusive use, more than one carrier can be used without the knowledge of the consignor or consignee. How is this expected to be handled? This needs to be more closely aligned with the P&TNSR. Section 4.2.1: Is there a certification a consignor can use to ensure carriers have a	For example: " As required by the *Packaging and Transport of Nuclear Substances Regulations*, the consignor **shall** provide the carrier with the appropriate transport documents relating to the shipment. In addition to the transport documents, the consignor shall include the corresponding description of security measures for sealed sources…." Bruce Power requests clarification on the questions and issues identified in the Industry Issue column.

Document section/excerpt of section	Industry issue	Suggested change
1. The package containing the sealed source **shall** be stored in a secure container. Packages over 500 kg are considered secure due to the handling difficulties caused by their weight. The secure container does not replace any other packaging or labeling required by any existing regulations. A secure container: a. **shall** be made of steel or any other material that is resistant to a physical attack by handheld tools b. **shall** be equipped with a key, combination padlock or similar locking device that is resistant to an attack using handheld tools c. if transported in an open conveyance (e.g., open back of a half-ton truck, flatbed truck), it **shall** be securely affixed to the vehicle to prevent unauthorized removal of the container d. if containing a sealed source with an activity level less than Category 3 (see Table A), may be stored in the securely locked trunk or other cargo area of a vehicle while in storage and during transportation 1. During a stopover while being transported, the package **shall** either be stored in a secure container in the vehicle (as described in list item 1, above), or in a location that is protected by physical security measures (as described in section 3). 2. The vehicle operator **shall** have on his or her person, at all times, a reliable mobile communication capability (e.g., cell phone) and a list of contact persons and their contact numbers in the event of an emergency situation. Alternate methodologies that provide a level of physical security equivalent to that described above may be	proven record for safety and security?	

Document section/excerpt of section	Industry issue	Suggested change
submitted to the CNSC for review, or identified in a licence application or a request to amend a licence. For transport of Category 1 or 2 sources and devices, the licensee **shall** verify that the carrier: - uses a package tracking system - implements methods to ensure trustworthiness and reliability of drivers - maintains constant control and/or surveillance during transit - has the capability for immediate communication to summon appropriate response or assistance For transport of Category 3 sources, the licensee **shall** verify that the carrier: - implements methods to ensure trustworthiness and reliability of drivers - maintains constant control and/or surveillance during transit - has the capability for immediate communication to summon appropriate response or assistance For transport of Category 4 and 5 sources, the licensee **shall** implement prudent management practices by using effective		
4.3 Transport security plan **4.3.1 Requirements for the transport security plan** In addition to the requirements in section 4.2.1, the following requirements apply to Category 1 and 2 sources:	Requirements for review of transportation security plan for Category 2 is unclear.	Bruce Power recommends the RD be revised to be clear regarding who must review the Category 2 transportation security plan; is it the CNSC or the licensee? And, define what is meant to "regular

Document section/excerpt of section	Industry issue	Suggested change
For transport of Category 1 sources, the licensee **shall** implement enhanced security measures and submit a specific Transport Security Plan to the CNSC at least 60 days before the anticipated date of shipment, for approval by the Commission Tribunal or a designated officer authorized by the Commission Tribunal For transport of Category 2 sources, the licensee **shall** implement enhanced security measures and develop a generic Transport Security Plan that **shall** be implemented and reviewed on a regular basis. The Transport Security Plan should be flexible to address changing threat levels, response protocols to a security event and the protection of sensitive information. For Category 1 sources, the Transport Security Plan **shall** include the following information: 1. the name, quantity, chemical/physical characteristics of the radioactive material 2. role and responsibilities of the licensee's personnel, consignors, carriers 3. mode(s) of transport 4. the proposed security measures 5. measures to monitor the location of the shipment 6. provisions for information security 7. communications arrangements made among the licensee, the carrier and the consignee 8. communications arrangements made with any police agency along the transportation route 9. the planned route alternate routes to be used in case of an emergency		basis" for the review of Category 2 sealed source response plans.