

Raymond N. Dickes  
Radiation Safety Officer  
Explosives Safety Officer

26  
**Schlumberger**

Secretary, U.S.  
Nuclear Regulatory Commission,  
Washington, DC 20555-0001  
Attn: Rulemakings and Adjudications Staff

DOCKETED  
USNRC

October 7, 2010 (4:42pm)

OFFICE OF SECRETARY  
RULEMAKINGS AND  
ADJUDICATIONS STAFF

Submitted via E-mail to: [Rulemaking.Comments@nrc.gov](mailto:Rulemaking.Comments@nrc.gov)

RE: Docket ID NRC-2008-0120

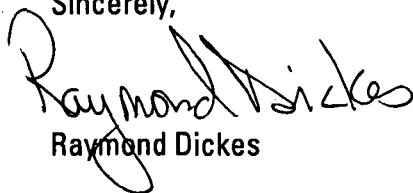
Dear Sirs:

Thank you for the opportunity to make comments on Docket ID NRC-2008-0120 regarding new proposed regulations for the security of radioactive materials. In the following pages you will find comments on specific subjects within the proposed rules (e.g. Reviewing Official). At the end of each subject are answers to questions for that subject that were directly posed by the Nuclear Regulatory Commission in Docket ID NRC-2008-0120. These questions are noted by a header of "NRC Questions" with the question numbered and shown in bold. For example:

1. **Is the local criminal history review necessary in light of the requirement for a FBI criminal history records check?)**

Thank you for the opportunity to make comments on Docket ID NRC-2008-0120.

Sincerely,

  
Raymond Dickes

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

### **Reviewing Official**

We question why the Reviewing Official needs to be reviewed and approved by the Nuclear Regulatory Commission (NRC) if Reviewing Officials are reviewed in the same manner, including fingerprints, as individuals granted unescorted access to Category 1 and or Category 2 quantities of radioactive materials? To our knowledge there have been no issues with the current system in which the Trustworthiness and Reliability Official in the Increased Control (IC) orders are reviewed and approved by a Trustworthiness and Reliability Official for the licensee.

Per the draft rules, Trustworthiness and Reliability Officials will be grandfathered and made Reviewing Officials. These individuals have been approving access to Category 1 and or Category 2 quantities of radioactive materials and will continue to do so when the rule is implemented. Granting access to Category 1 and or Category 2 quantities of radioactive materials requires the same level of trustworthiness and reliability as approving another person as a Reviewing Official who may then in turn grant access to Category 1 and or Category 2 quantities of radioactive materials.

This proposed rule adds an unnecessary review with no benefit.

### **NRC Questions**

1. Does the reviewing official need to be fingerprinted and have a FBI criminal records check conducted?

Yes. Reviewing Officials should be reviewed in the same manner as individuals granted unescorted access to Category 1 and or Category 2 quantities of radioactive materials since the Reviewing Officials will be reviewing and approving these individuals. However, referring to our comment above on the Reviewing Official, we do not believe the Reviewing Official needs to be reviewed and approved by the Nuclear Regulatory Commission (NRC).

2. Are the other aspects of the background investigation adequate to determine the trustworthiness and reliability of the reviewing official?

We believe that Reviewing Officials should be reviewed in the same manner as individuals granted unescorted access to Category 1 and or Category 2 quantities of radioactive materials. However, our experience with the various checks required by the IC orders shows that only the criminal history check has value in determining trustworthiness and reliability. Schlumberger has reviewed 3,182 persons since the IC Fingerprint Order was implemented, which is, according to statements made by the NRC at a public meeting on September 1, 2010 in Austin, Texas, approximately 7% of all persons fingerprinted as per this order., Schlumberger has determined

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

that 38 of these 3,182 persons could not be judged trustworthy and reliable. None of these decisions were based on the education verification, previous employment verification, personal reference checks, or any other aspect of the person that was reviewed other than the criminal history check. For all 38 persons that were judged to be not trustworthy and reliable, the decision was based on criminal history identified in the report from the Federal Bureau of Investigation.

More than 90% of these persons that were judged to be trustworthy and reliable, also were judged to be trustworthy and reliable by the Bureau of Alcohol, Tobacco, Firearms and Explosives (BATFE). This experience appears to validate why all other federal agencies (e.g. BATFE) that perform similar checks and determination do so solely on the basis of criminal history derived from the Federal Bureau of Investigation.

### **3. Are there other methods that could be used to ensure that the reviewing official is trustworthy and reliable?**

Trustworthiness and Reliability Officials, and in the future Reviewing Officials, generally are more senior employees of the licensee and thus have extensive history with the licensee. This history is a far more accurate set of data for determining trustworthiness and reliability than any other check proposed. Per the draft rules, this employment history appears to have been completely ignored and is a major change from the IC orders. In the IC orders, all checks other than the fingerprint-based criminal history check were not required for an employee with more than 3 years employment with the licensee. In addition, in the IC orders, employment history is a factor that can be used when determining whether an employee with criminal history is trustworthy and reliable.

### **4. Is fingerprinting Reviewing Officials too large a burden?**

The fingerprinting of the reviewing official is not too large a burden. Reviewing officials should be reviewed in the same manner as individuals granted unescorted access to Category 1 and or Category 2 quantities of radioactive materials since the reviewing officials will be reviewing and approving these individuals.

## **Background Investigation for Trustworthiness and Reliability Determination**

We believe that the background investigation for trustworthiness and reliability determination should only require a fingerprint-based criminal history check and that adverse criminal history may be mitigated by the employment history of an employee with more than 3 years employment with the licensee.

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

---

Schlumberger has reviewed 3,182 persons since the IC Fingerprint Order was implemented, which is, according to statements made by the NRC at a public meeting on September 1, 2010 in Austin, Texas, approximately 7% of all persons fingerprinted as per this order. Schlumberger has determined that 38 of these 3,182 persons could not be judged trustworthy and reliable. None of these decisions were based on the education verification, previous employment verification, personal reference checks, or any other aspect of the person that was reviewed other than the criminal history check. For all 38 persons who were judged to be not trustworthy and reliable, the decision was based on criminal history identified in the report from the Federal Bureau of Investigation.

More than 90% of these persons who were judged to be trustworthy and reliable also were judged to be trustworthy and reliable by the Bureau of Alcohol, Tobacco, Firearms and Explosives (BATFE). This experience appears to validate why all other federal agencies (e.g. BATFE) that perform similar checks and determinations do so solely on the basis of criminal history derived from the Federal Bureau of Investigation.

However, employment history is a far more accurate set of data for determining trustworthiness and reliability than any other check proposed. Employees with extended service, more than 3 years employment with the licensee, in general are trusted with authority and responsibility for valuable assets, money, purchasing power, etc. in addition to unescorted access to Category 1 and or Category 2 quantities of radioactive materials. This employment history should not be ignored.

This experience appears to validate why other federal agencies (e.g. Bureau of Alcohol, Tobacco, Firearms and Explosives) that perform checks and determination on the basis of criminal history derived from the Federal Bureau of Investigation, also make favorable determinations in spite of criminal history based on their personal and employment history.

Per the draft rules, this employment history appears to have been completely ignored and is a major change from the IC orders. In the IC orders, all checks other than the fingerprint-based criminal history check were not required for an employee with more than 3 years employment with the licensee. In addition, in the IC orders, employment history is a factor that can be used when determining whether an employee with criminal history is trustworthy and reliable.

### **NRC Questions**

2. Is the local criminal history review necessary in light of the requirement for a FBI criminal history records check?

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

---

This check is redundant and does not add any value. As previously noted, Schlumberger has reviewed 3,182 persons since the IC Fingerprint Order was implemented. A federal, state and local criminal history check using a private investigator was performed on each of these individuals. In all 3,182 cases, all information identified by the federal, state and local criminal history check using a private investigator was also contained in the fingerprint-based criminal history derived from the Federal Bureau of Investigation.

### **3. Does the credit history check provide valuable information for the determination of trustworthiness and reliability?**

We do not believe that a credit history check provides valuable information for the determination of trustworthiness and reliability. We believe that any data used for the determination of "Trustworthiness" needs to meet at least these three criteria since a person's ability to work will likely be determined in part by this data:

1. The data must be accurate;
2. The Reviewing Officials must be able to easily, consistently and fairly relate the data to a person's trustworthiness and reliability; and
3. The cost of performing the data collection plus the trustworthiness and reliability review and determination must have a benefit that is consistent with the costs.

My review of the use of credit history as part of the determination of a person's "Trustworthiness" shows that the use of credit history does not meet any of the three criteria above.

The accuracy of the information in Credit Reporting Databases has been called into question in numerous studies. According to "Fair Credit Reporting", published by the National Consumer Law Center, Inc. in 2006, the credit reporting systems have an error rate greater than 70% and greater than 25% of all reports contain "an error serious enough to cause a denial of credit".

This shockingly high error rate has been noted in numerous studies and was "the primary theme throughout all legislative debates leading up to the FCRA," as reported in "Fair Credit Reporting". "Fair Credit Reporting" cites studies conducted in 1998, 2000, 2002 and 2004 which all identified serious problems with the accuracy of information in the Credit Reporting Databases. These studies show that no improvement occurred in the accuracy of the data during the period from 1998 to 2004. Even if the accuracy has improved in recent years, it is unlikely that the error rate has been reduced to an acceptable level.

Two arguments used to support the use of credit history are:

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

---

1. That a person with "bad" credit history may be a security risk since they are more susceptible either to directly stealing a radioactive source for personal profit or to bribes from a third party for their assistance in stealing a radioactive source; and
2. That a person without credit history may not be who they claim to be and thus may be a security risk.

Based on a review I conducted with a Fair Credit Reporting agency, I believe that items 1 and 2 above cannot be determined from the type of data or lack of data in a credit history.

The data in a credit report cannot be easily, consistently and fairly related to a person's "Trustworthiness". This credit history data may consist of one or more of the items as follows:

- A foreclosure on a home mortgage;
- A credit account closed at the request of the credit grantor;
- An open credit account (e.g. home mortgage, credit card, school loan, etc.) with an outstanding balance for which payments have stopped, were never started or are delinquent.

When the population that will be reviewed is considered along with the data, assessing "Trustworthiness" will not be easy, will not be consistent and likely will result in the process being unfair. This assumes that the data is accurate which is strongly questioned. In the specific example of Schlumberger, more than 90% of the population that will be evaluated will be less than 25 years old and one of the following:

- A recent college graduate;
- A recently discharged member of the armed forces of the U.S.; or
- A high school graduate seeking a job with career opportunities.

The age of this population and their status matters since:

1. This age group on average will have the smallest previous incomes and potentially very large debts (e.g. school loans)
2. This age group on average has the lowest credit scores and the least experience with managing money. A credit reporting company may report most negative information for seven years. Thus youthful mistakes that do not correlate to "Trustworthiness" will still be on their record; and
3. A recent college graduate who received grants and scholarships may have no credit history at all.

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

---

These factors taken together argue that, even when accurate information is available, the expected wide range of credit history results makes the relationship of this data to "Trustworthiness" at best nebulous and at worst meaningless.

The cost of hiring a credit reporting agency to provide the history, of evaluating this data, and to handle cases of erroneous data, is substantial and the benefits appear to be extremely small.

The potential benefit is the prevention of a theft of a radioactive source. Schlumberger has been using radioactive sources since 1950, and in that sixty year period (more than ½ a century), Schlumberger has never had an attempted theft of a radioactive source nor a radioactive source stolen. This successful record likely results from a variety of factors, including good candidate selection, frequent evaluation of job performance, and long-term job opportunities within the company. This results in a loyal and motivated employee population.

As I have already discussed, the accuracy of the information in Credit Reporting Databases has been called into question. Unfavorable decisions made using inaccurate data will directly and negatively affect our employee population and thus the forced use of this data could result in not only no benefits but could, and likely will, cause harm to an already successful program.

The total cost of adding a "Trustworthiness" program using credit data will be substantial. Schlumberger currently averages approximately 1,000 new hires per year who require a "Trustworthiness" determination. Our estimate is that it will cost \$150 per person to collect the credit data and attempt to use the data in our "Trustworthiness" evaluation. This is \$150,000 per year which will likely result in no benefits and could cause harm.

I believe that the evaluation of credit history does not offer a useful tool in determining "Trustworthiness" since the accuracy of the information in Credit Reporting Databases has been called into question, the data cannot be easily, consistently and fairly related to a person's "Trustworthiness", and it appears the costs of using this data are substantial with no benefits and possible negative side effects.

### **3. What are the appropriate elements of a background investigation and why are any suggested elements appropriate?**

Based on our review of 3,182 persons since the IC Fingerprint Order was implemented, we believe that the background investigation for trustworthiness and reliability determination should only require a fingerprint-based criminal history check and that adverse criminal history may be mitigated by satisfactory employment history of more than 3 years with the licensee.

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

---

### **4. Are the elements of the background investigation too subjective to be effective?**

Based on our experience in reviewing 3,182 persons since the IC Fingerprint Order was implemented, we have found that with the exception of the private investigator criminal history check and fingerprinted-based criminal history check, all of the other proposed elements are either too subjective and thus cannot be easily, consistently and fairly related to a person's trustworthiness and reliability or are both inaccurate and too subjective.

### **5. How much time does a licensee typically spend on conducting the background investigation for an individual?**

Based on our experience in reviewing 3,182 persons since the IC Fingerprint Order was implemented, approximately three man-days on average is required to complete the education verification, previous employment verification, personal reference checks, private investigator criminal history check and fingerprinted-based criminal history check. This time could be reduced by over 80% with no decrease in effectiveness if only fingerprinted-based criminal history checks were required.

### **Local Law Enforcement Agencies (LLEA) Coordination and Notification of Work at Temporary Job Sites**

Coordination with the LLEAs that have jurisdiction over our operating bases does not add any value based on our experience with LLEAs gained during our coordination requests required under the ICs. Since the ICs were implemented, we have had operating bases in fifty separate jurisdictions in nineteen states. In none of these cases was the coordination with the LLEA beneficial. At best the LLEA would acknowledge our coordination attempts with no commitments from them other than to respond in the manner they believed was proper. Most LLEAs were completely disinterested and did not acknowledge any information provided to them.

In the proposed rules, the requirement for coordination with the LLEA is expanded in scope for LLEAs that have jurisdiction over our operating bases to include a request for commitments from the LLEAs. Clearly the NRC understands that the coordination with the LLEAs under the ICs was not successful since the proposed rules now include a reporting requirement to the NRC if the LLEA either does not respond to communication from the licensee within 60 days or refuses to agree with request for commitments from the LLEAs by licensees.

However, the proposed rules appear to ignore the root cause of why the coordination with the LLEAs under the ICs was not successful and instead proposes a burdensome reporting requirement that could poison the licensee's relationship with the LLEA. In our discussions with those LLEAs where feedback was provided, the LLEAs were unwilling to discuss the manner in



## **Comments on NRC Proposed Security Rules (10 CFR 37)**

which they planned to respond and unwilling to commit to any specific action. They believe each decision to respond must be based on their judgment of the circumstance as each request for response occurs. Adding a reporting requirement does not address this root cause.

We annually perform approximately 50,000 well logging operations at temporary job sites in 27 states and offshore in the Gulf of Mexico. Even though many of these operations can be completed in less than seven days, at least 5,000 of these operations will require, under the proposed rules, a notification to the LLEA with jurisdiction at least three days in advance of the start of operations. Other operations that initially were expected to be completed in less than seven (7) days will experience delays that are beyond the control of the logging company (e.g. deteriorating well conditions that require fishing for logging tools).

This is over 14 notifications per day to hundreds, if not thousands, of LLEAs during a single year for one well logging company. This will be increased to hundreds of notices per day when all well logging companies are considered and increased for other types of operations.

This blizzard of paper will be time-consuming to produce and, if it is to be valuable, time-consuming for LLEA's to read and comprehend.

### **NRC Questions**

**1. Is there any benefit in requiring that the LLEA be notified of work at temporary job sites?**

No. Coordination with the LLEAs that have jurisdiction over temporary job sites will not add any value based on our experience with LLEAs gained during our coordination requests required under the ICs.

**2. Should notifications be made by licensees for work at every temporary job sites or only those where the license will be working for longer periods, such as the 7 day timeframe proposed in the rule?**

No. Coordination with the LLEAs should not be a requirement for operations at any temporary job site.

**3. If notifications are required, is 7 days the appropriate threshold for notification of the LLEA or should there be a different threshold?**

No. Coordination with the LLEAs should not be a requirement for operations at any temporary job site but if notification is required, thirty days appears to be a more appropriate timeframe. This would limit the number of notifications to manage and make any notifications received by the LLEA's more meaningful.

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

### **4. Will licensees be able to easily identify the LLEA with jurisdiction for temporary job sites or does this impose an undue burden?**

No. For well logging operations the LLEA with jurisdiction for temporary job sites will not be readily identifiable from well identification information. With approximately 50,000 well logging operations at temporary job sites in 27 states and offshore in the Gulf of Mexico, this means that a burdensome process to identify thousands of LLEA's will be required. For example, questions will occur such as:

- A well is in a specific county, but is it within the city limits of a specific town or city? In this case, who is the appropriate LLEA?
- Who is LLEA for offshore operations?
- A well is in a specific county, but is it within the jurisdiction of tribal police on a reservation?

It will be time-consuming to identify the LLEA and without meaningful benefit.

### **5. Are LLEAs interested in receiving these notifications?**

Based on our experience with LLEAs gained during our coordination requests required under the ICs, LLEAs with jurisdiction over temporary job sites will not be interested in any information provided to them.

## **Physical Security During Transit**

### **NRC Questions**

#### **1. Should relief from the vehicle disabling provisions be provided?**

Schlumberger has not experienced any attempts to steal vehicles containing radioactive materials. Based on our experience, the addition of security beyond the normal security provided by the removal of the ignition key is not warranted and unnecessary. We support removal of the vehicle disabling requirements.

#### **2. Have licensees experienced any problems in implementing this aspect of the Increased Controls?**

The use of vehicle-disabling devices is not difficult but does add an expense and makes the removal of vehicles in the event of an emergency more difficult. Based on our experience, the addition of security beyond the normal security provided by the removal of the ignition key is not warranted and unnecessary.

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

---

3. Should there be an exemption written into the regulations or should licensees with overriding safety concerns be required to request an exemption from the regulations to obtain relief from the provision?

Based on our experience, the addition of security beyond the normal security provided by the removal of the ignition key is not warranted and unnecessary. The use of vehicle-disabling devices adds an expense and makes the removal of vehicles in the event of an emergency more difficult. We believe that the vehicle-disabling requirement should be removed without requirement for an exemption.

4. If an exemption is included in the regulations, should it be a blanket exemption or a specific exemption for the oil and gas industry?

In order of preference, we believe that:

- The vehicle disabling requirement should be removed without requirement for an exemption; or
- A blanket exemption should exist within the regulations; or
- A specific exemption for vehicles used in the oil and gas industry should exist within the regulations.

Based on our experience, the addition of security beyond the normal security provided by the removal of the ignition key is not warranted and unnecessary. The use of vehicle disabling devices adds an expense and makes the removal of vehicle in the event of an emergency more difficult.

5. Does the disabling provision conflict with any Occupational Safety and Health Administration requirements or any State requirements?

The body of local, state and federal regulations on occupational safety is extremely large and complex. An exhaustive search of these regulations is not possible in a short period of, but vehicle-disabling devices make the removal of vehicles in the event of an emergency more difficult and likely at least contrary to the spirit of some of these regulations.

### **Event Reporting**

10 CFR § 37.57 Reporting of events, contains a requirement to report to the NRC Operations Center five types of events:

- Actual theft of category 1 or category 2 quantities of radioactive material;
- Attempted theft of category 1 or category 2 quantities of radioactive material;

## Comments on NRC Proposed Security Rules (10 CFR 37)

---

- Sabotage;
- Diversion of category 1 or category 2 quantities of radioactive material; and
- Any suspicious activity related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material.

Classifying some of these events will be very subjective and some are likely to be impossible to distinguish from events that are not malicious or are not related to category 1 or category 2 quantities of radioactive material. With this being the case, managing these requirements will be difficult since reasonable persons could interpret the expectations of the NRC and the details of a specific event very differently. In addition, it is not clear that the NRC understands most of these events will require a period of assessment, and sometimes a lengthy period of assessment, to determine the nature of the event.

Of these events, "Actual and attempted theft of category 1 or category 2 quantities of radioactive material" are not uniquely defined in 10 CFR § 37. However, these events are likely to be the most easily interpreted and be the easiest to assess. However, if a discrepancy in the inventory is discovered without any evidence of an "actual theft" (e.g. locks that have been cut), a period of assessment will be required to determine the nature of the event. The proposed timeframes for reporting (e.g. "*immediate*") do not anticipate a period of assessment.

As defined in 10 CFR § 37; "*Sabotage means deliberate damage, with malevolent intent, to a category 1 or category 2 quantity of radioactive material, a device that contains a category 1 or category 2 quantity of radioactive material, or the components of the security system.*" It is difficult to see how a licensee can be expected to determine that any act is sabotage since the definition includes knowing the "intent" of the person causing the damage and whether their intent is "malevolent". Since it is not possible for a licensee to determine "intent", this requirement should be removed.

As is defined in 10 CFR § 37; "*Diversion means the unauthorized movement of radioactive material subject to this part to a location different from the material's authorized destination inside or outside of the site at which the material is used or stored.*". It is not clear what the NRC's expectations are concerning diversion. If category 1 or category 2 quantities of radioactive material are moved and this movement is unauthorized, how does this differ from a theft? To be effectively implemented, less subjective requirements are needed.

Suspicious activity is not defined in 10 CFR § 37. Based on the definition found in a dictionary of "suspicious", a reasonable person could define "suspicious activity" as; *An activity that causes one to have the idea or impression that the activity is questionable, illegal, dishonest, or dangerous.* Based on this definition, judging an activity as suspicious will be very subjective. A legal activity (e.g. photographing a facility where category 1 or category 2 quantities of radioactive material are stored) might be interpreted as "questionable" and thus "suspicious" by one person but not by another person. It is not clear what the NRC's expectations are concerning suspicious activity. If a person is seen photographing a facility where category 1 or category 2

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

---

quantities of radioactive material are stored, is this a suspicious activity? To be effectively implemented, less subjective requirements are needed.

### **NRC Questions**

#### **1. Are these the appropriate items and thresholds to be reported to the LLEA?**

Sabotage, diversion and any suspicious activity related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material are not appropriate items and thresholds for reporting. Actual and attempted theft of category 1 or category 2 quantities of radioactive material the answer are appropriate items and thresholds for reporting.

#### **2. Are these the appropriate items and thresholds to be reported to the NRC?**

No for sabotage, diversion and any suspicious activity related to possible theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material but absolutely yes for actual and attempted theft of category 1 or category 2 quantities of radioactive material.

#### **3. Should suspicious activities be reported? If they are reported, what type of activities should be considered suspicious?**

Suspicious activity is not an appropriate item and threshold for reporting. Suspicious activity is not defined in 10 CFR § 37. Based on the definition found in a dictionary of "suspicious", a reasonable person could define "suspicious activity" as; *An activity that causes one to have the idea or impression that the activity is questionable, illegal, dishonest, or dangerous.* Based on this definition, judging an activity as suspicious will be very subjective. A legal activity (e.g. photographing a facility where category 1 or category 2 quantities of radioactive material are stored) might be interpreted as "questionable" and thus "suspicious" by one person but not by another person. It is not clear what the NRC's expectations are concerning suspicious activity. If a person is seen photographing a facility where category 1 or category 2 quantities of radioactive material are stored, is this a suspicious activity? To be effectively implemented, less subjective requirements are needed.

#### **4. Is the timeframe for reporting appropriate?**

The proposed timeframes for reporting are not appropriate since they do not allow for a realistic period of assessment. In § 37 .57(a) the proposed timeframes are "*immediate*" to the LLEA and "*In no case shall the notification to the NRC be later than 4 hours after the discovery of any attempted or actual theft, sabotage, or diversion*". In § 37 .57(b), the proposed timeframes are effectively the same as § 37 .57(a) with "*upon discovery*" to the LLEA and "*but not later than 4 hours after notifying the LLEA*" for the report to the NRC.

Classifying some of these events will be very subjective and some are likely to be impossible to distinguish from events that are not malicious or are not related to category 1 or category 2

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

quantities of radioactive material. With this being the case, managing these requirements will be difficult since reasonable persons could interpret the details of a specific event very differently.

The words "immediate" and "upon discovery" suggest that the licensee must make a snap judgment on the nature of the event and no time allowed to assess the situation. As written, most of the events listed in the proposed regulations will require a period of assessment to determine the nature of the event. If this is not the intent of the NRC, the terms "immediate" and "upon discovery" should be changed to indicate that the notifications are required after the licensee assesses and concludes that a reportable event has taken place.

### **Licensee Verification for Transfers**

The licensee verification requirement may have an unintended consequence and we urge the NRC to clarify this requirement. The requirement in § 37.71(b) appears to imply a licensee-verification requirement for any movement of Category 2 amounts of radioactive materials where the agency (NRC or Agreement State) with jurisdiction over the point of origin of the shipment is different from the agency with jurisdiction over the destination. For a single legal entity with operations in multiple states or operating offshore in federal waters, shipments that result in a change of jurisdiction but without a change of licensee will frequently occur. For example, Schlumberger may ship a Category 2 amount of radioactive materials from Louisiana to a temporary job site under the jurisdiction of the Nuclear Regulatory Commission. Though the governing license changed, the licensee did not. A license verification should not be required in these cases and the NRC needs to clarify § 37.71(b).

### **NRC Questions**

1. **Should there be a requirement for verification of the license for transfers of category 2 quantities of radioactive materials or would it be acceptable to wait for the system being developed before requiring license verification for transfers of category 2 quantities of radioactive materials?**

Waiting on the system being developed before requiring license verification for transfers of category 2 quantities of radioactive materials is sensible and recommended. In addition, license verification should not be required for shipments that result in a change of jurisdiction but without a change of licensee.

2. **We are interested in how address verification might work for shipments to temporary job sites and the ability of both licensees and Agreement States to comply with such a requirement. For example, would States be able to accommodate such requests with their current record systems?**

## **Comments on NRC Proposed Security Rules (10 CFR 37)**

---

For well logging operations in the oil and gas industry, address verification for shipments to temporary job sites is not possible. Oil and gas drilling sites do not have addresses and are identified by well identification (e.g. API #) and coordinates.

- 3. We are also seeking comment on the frequency of the license verification. For example, should a licensee be required to check with the licensing agency for every transfer or would an annual check (or some other frequency) of the license be sufficient?**

We believe that license verification should not be required for shipments that result in a change of jurisdiction but without a change of licensee. The license system should be set up so that each licensee can annually validate the license of another licensee and subscribe to this licensee. The subscriber could then:

- Be notified if a substantial change on this license occurs that would then require a new validation; or
  - If no notifications are received because no substantial changes have occurred, continue to make shipments for one year until a new validation is required. The system could notify the subscriber that the annual verification is due.
- 4. If an annual check is allowed, how would the transferring licensee know if a license has been modified since the last check and that the licensee is still authorized to receive the material?**

We believe that license verification should not be required for shipments that result in a change of jurisdiction but without a change of licensee. The license system should be set-up so that each licensee can annually validate the license of another licensee and subscribe to this licensee. The subscriber could then:

- Be notified if a substantial change on this license occurs that would then require a new validation; or
- If no notifications are received because no substantial changes have occurred, continue to make shipments for one year until a new validation is required. The system could notify the subscriber when an annual verification is due.

- 5. Is preplanning and coordination of the shipments necessary?**

Coordination with the receiving licensee for category 2 quantities of radioactive materials is sensible and recommended.

## Rulemaking Comments

---

**From:** Raymond Dickes [dickes1@slb.com]  
**Sent:** Thursday, October 07, 2010 3:53 PM  
**To:** Rulemaking Comments  
**Subject:** Comments for Docket ID NRC-2008-0120  
**Attachments:** Comments on 10CFR37.pdf

Dear Sirs,

Attached are comments for Docket ID NRC-2008-0120.

Regards,

Ray Dickes



Received: from mail1.nrc.gov (148.184.176.41) by TWMS01.nrc.gov  
(148.184.200.145) with Microsoft SMTP Server id 8.1.393.1; Thu, 7 Oct 2010  
15:53:29 -0400

X-Ironport-ID: mail1

X-SBRS: 5.3

X-MID: 23804928

X-fn: Comments on 10CFR37.pdf

X-IronPort-AV: E=Sophos;i="4.57,298,1283745600";

d="pdf?scan'208,217";a="23804928"

Received: from sx003.ddc-nl0105.slb.com (HELO nl0105mta01.mail.slb.com)  
([199.6.196.58]) by mail1.nrc.gov with ESMTP; 07 Oct 2010 15:53:08 -0400

Received: from nl0105mta01.mail.slb.com (localhost.localdomain [127.0.0.1]) by  
localhost (Postfix) with SMTP id DFC9159024B for

<Rulemaking.Comments@nrc.gov>; Thu, 7 Oct 2010 19:53:05 +0000 (GMT)

Received: from NL0230MBX01N2.DIR.slb.com (nl0230mbx01n2.dir.slb.com  
[199.6.133.5]) (using TLSv1 with cipher AES128-SHA (128/128 bits)) (No client

certificate requested) by nl0105mta01.mail.slb.com (Postfix) with ESMTPS id

234A85902A3 for <Rulemaking.Comments@nrc.gov>; Thu, 7 Oct 2010 19:53:05

+0000 (GMT)

Received: from NL0230MBX10N1.DIR.slb.com (199.6.132.23) by  
NL0230MBX01N2.DIR.slb.com (199.6.133.5) with Microsoft SMTP Server (TLS) id  
14.0.639.21; Thu, 7 Oct 2010 21:53:04 +0200

Received: from NL0230MBX09N2.DIR.slb.com ([169.254.2.67]) by  
NL0230MBX10N1.DIR.slb.com ([169.254.1.115]) with mapi; Thu, 7 Oct 2010  
21:53:03 +0200

From: Raymond Dickes <dickes1@slb.com>

To: "Rulemaking.Comments@nrc.gov" <Rulemaking.Comments@nrc.gov>

Subject: Comments for Docket ID NRC-2008-0120

Thread-Topic: Comments for Docket ID NRC-2008-0120

Thread-Index: ActmWTWZ2s8Auv57QuGMc84+pHWEgg==

Date: Thu, 7 Oct 2010 19:52:44 +0000

Message-ID:

<A1AD5BCF83FC674CB869B52839A3E591058C1B5A@NL0230MBX09N2.DIR.slb.com>

Accept-Language: en-US

Content-Language: en-US

X-MS-Has-Attach: yes

X-MS-TNEF-Correlator:

Content-Type: multipart/mixed;

boundary="\_004\_A1AD5BCF83FC674CB869B52839A3E591058C1B5ANL0230MBX09N2DI\_"

MIME-Version: 1.0

Return-Path: dickes1@slb.com