PHMSA DIMP Inspection Form Version 9-23-11 and a Discussion of How Each Item Is Addressed In a Written DIMP Plan Created Using SHRIMP

The following items are included on the inspection form that Pipeline and Hazardous Materials Safety Administration (PHMSA) and the states have developed for auditing compliance with the DIMP rule. The numbers shown are the question numbers from the inspection form (Questions 1 and 2 are omitted because they are simple). Each question begins with either a reference to the section of 49 CFR Part 192 Subpart P Distribution Integrity Management Programs regulations where the requirement addressed in the question can be found (e.g.".1007(a)(1)") or "Information Only" if the question asks for something not specifically required by Subpart P.

Inspection Form Questions

3. (Information Only) Does the operator's plan assign responsibility, including titles and positions, of those accountable for developing and implementing required actions?

The SHRIMP written plan includes an attachment "Implementation Plan". The SHRIMP User's Guide and guidance within SHRIMP advise the user that the above information is expected to be included in the Implementation Plan.

4. .1007(a)(1) Do the written procedures identify or reference the appropriate sources used to determine the following characteristics necessary to assess the threats and risks to the integrity of the pipeline:
    a. Design (e.g. type of construction, inserted pipe, rehabilitated pipe method, materials, sizes, dates of installation, mains and services, etc.)?
    b. Operating Conditions (e.g. pressure, gas quality, etc.)?
    c. Operating Environmental Factors (e.g. corrosive soil conditions, frost heave, land subsidence, landslides, washouts, snow damage, external heat sources, business districts, wall-to-wall paving, population density, difficult to evacuate facilities, valve placement, etc.)?

SHRIMP includes a Data Source field in each interview screen in which the user can enter a description of the source of information used to answer each question. The text entered by the user is included in the attachment to the plan showing the answers provided by the user to each interview question.

SHRIMP interview questions are based on the Gas Piping Technology Committee (GPTC) guidance and supplemented with additional questions developed by the

government/industry SHRIMP) Advisors group. There are questions within each threat assessment addressing design, operating conditions and operating environment.

Not all the examples listed were included in SHRIMP interview questions. Some were felt not to have significant bearing on risk (e.g. inserted pipe, age, date of installation). Others are addressed indirectly (e.g. soil corrosivity can be inferred by answers to questions about corrosion leak history, exposed pipe inspections and pipe-to-soil potentials. Since operators are not required to measure soil corrosivity operators were not expected to have this information).

Many of the listed items apply to specific threats (e.g. gas quality only to internal corrosion).

While SHRIMP may not ask for each and every data element listed in the examples, the SHRIMP User's Guide offers these as examples of additional information the user should consider when validating SHRIMP's risk rankings.

5. .1007(a)(2) Do the written procedures require the consideration of information gained from past design, operations, and maintenance (e.g. O&M activities, field surveys, One-Call system information, excavation damage, etc.)?

Yes. All of the examples are information used by SHRIMP in one or more of the threat assessments.

6. (Information Only) Do the written procedures indicate if the information was obtained from electronic records, paper records, or subject matter expert knowledge (select all which apply)?

The SHRIMP User's Guide urges users to include this in the Data Source field, which is written into the plan for each question in Chapter 11.2

7. .1007(a)(3) Does the plan contain written procedures to identify additional information that is needed to fill gaps due to missing, inaccurate, or incomplete records?
8. .1007(a)(3) Does the plan list the additional information needed to fill gaps due to missing, inaccurate, or incomplete records?
9. .1007(a)(3) Do the written procedures specify the means to collect the additional information needed to fill gaps due to missing, inaccurate, or incomplete records (e.g., O&M activities, field surveys, One-Call System, etc.)?

Written procedures are included in the Procedures Attachment (11.3). If the user answered "I don't know" to any question where that is an option, the user is asked to either select text prewritten by SHRIMP or substitute text written by the user listing the missing information and describing how the information will be collected. That will be found in the Implementation Plan attachment to the written plan (11.1).

10. .1007(a)(5) Do the written procedures require the capture and retention of data on any new pipeline installed?
11. .1007(a)(5) Does the data required for capture and retention include, at a minimum, the location where the new pipeline is installed and the material from which it is constructed?

Yes, in Chapter 3 the plan states that this information will be captured and retained. The user is asked to provide a description of the process to capture and retain this information in the Attachment labeled "Implementation Plan." Chapter 11.1

12. .1007(a) Does the documentation provided by the operator demonstrate implementation of the element "Knowledge of the System"?
13. .1007(a) Has the operator demonstrated an understanding of its system?

Knowledge is required to answer the interview questions in SHRIMP. Additional knowledge above and beyond that asked for in SHRIMP interviews can and should be applied by the user in the risk ranking validation process.

14. .1007(b) In identifying threats, do the written procedures include consideration of the following categories of threats to each gas distribution pipeline?
    a. Corrosion
    b. Natural Forces
    c. Excavation Damage
    d. Other Outside Force Damage
    e. Material or Welds
    f. Equipment Failure
    g. Incorrect Operation
    h. Other Concerns

Yes

15. .1007(b) Did the operator consider the information that was reasonably available to identify existing and potential threats?

Most of the questions asked by SHRIMP can be answered from records of inspection and maintenance required by 49 CFR Part 192, therefore it should be reasonably available.

SHRIMP questions address both actual and potential threats. Questions about leak history by cause, observations of metal loss due to corrosion, etc are addressing actual threats. Questions about conditions that could lead to failures, even if no failures have actually occurred, are addressing potential threats. Some examples of the latter are pipe-to-soil readings, stray currents, increase in locate requests, pipe located in areas of known earth movement, etc.

16. (Information Only) Does the plan subdivide the primary threats into subcategories to identify existing and potential threats?

Yes. SHRIMP requires the user to consider subthreats. For example, corrosion includes 3 subthreats – external, internal and atmospheric.

17. .1007(b) In identifying threats did the information considered include any of the following?
    a. Incident and leak history -- *yes*
    b. Corrosion control records -- *yes*
    c. *Continuing surveillance records -- not directly**
    d. Patrolling records -- *yes*
    e. Maintenance history -- *yes*
    f. Excavation damage experience -- *yes*
    g. Other – Describe -- *A complete list of information required by SHRIMP is attached.*

*SHRIMP does not ask for records of continuing surveillance, as continuing surveillance is not an inspection but rather a process of integrating and evaluating all known information about the pipeline resulting from inspection and maintenance activities.

18. (Information Only) Does the plan categorize primary threats as either "system-wide" or "localized"?

If the user answers questions in a manner that indicates there may be a problem, SHRIMP asks if the problem is system-wide or concentrated. "Concentrated" as used in SHRIMP means the same as "localized" in the audit form.

19. (Information Only) Do the written procedures consider, in addition to the operator's own information, data from external sources (e.g. trade associations, government agencies, or other system operators, etc.) to assist in identifying potential threats?

The SHRIMP risk model considers national level experience on leak repairs by cause and reportable incidents by cause. SHRIMP cross references PHMSA advisory bulletins and PPDC information, where such information is pertinent to any threat. For example, under Material defect threat there is a link to the three PHMSA advisory bulletins about brittle like cracking in certain plastics.
Planned enhancements to SHRIMP include using material-specific leak data entered by SHRIMP users to determine the mean and standard deviation of leaks repaired per mile and per service by cause and by type of materials (e.g. coated, cathodically-protected steel) that will improve the threat assessment and risk ranking. SHRIMP data will also be evaluated for trends in failures with particular types of equipment. All this information will be provided to SHRIMP users to improve their DIMP programs.

20. .1007(b) Does the documentation provided by the operator demonstrate implementation of the element "Identify Threats"?

SHRIMP records all the major decisions made by the user and summarizes these in Chapter 4 of the written plan titled "THREAT ASSESSMENT."

All answers provided by users are shown in an attachment to the Plan (11.2). These document the implementation of "Identify Threats"

21. (Information Only) Was the risk evaluation developed fully or in part using a commercially available tool?

If you're reading this, the user most likely fully or partially used SHRIMP.

22. .1007 (c) Do the written procedures contain the method used to determine the relative importance of each threat and estimate and rank the risks posed? Briefly describe the method.

The SHRIMP Risk ranking model assigns numeric scores to questions related to the probability of a failure due to each threat. Relative weightings are based on subject matter expert consensus (e.g. the SHRIMP Advisors). Probability scores are normalized to 1-10. A consequence factor is determined based on answers to questions about consequence. This is multiplied by the probability score. A leak history factor is

determined according to the fraction of leak repairs by threat on the operator's system over the past three years (e.g if 25% of the operator's leak repairs were corrosion leaks, corrosion threats would get a 25% boost in risk score). Finally, an incident factor is applied, based on the relative probability a failure would result in death, injury or significant property loss (e.g. result a reportable incident). Excavation, incorrect operation and natural force damage threats receive a 25% boost in relative risk ranking. The model is described more completely in the attached.

23. .1007 (c) Do the written procedures to evaluate and rank risk consider each applicable current and potential threat?

Procedures are described in the "Procedures" attachment to the written plan.

24. 1007 (c) Do the written procedures to evaluate and rank risk consider the likelihood of failure associated with each threat?

Each threat assessment, with the exception of "Other Threats," includes questions addressing the likelihood of a failure due to that threat. When the user identifies threats under "Other" SHRIMP guidance asks the user to consider likelihood, but since there is no way to know what "Other" may be SHRIMP cannot assist by asking specific questions.

25. 1007 (c) Do the written procedures to evaluate and rank risk consider the potential consequence of such a failure?

Each threat assessment, with the exception of "Other Threats," includes questions addressing the consequences of a failure due to that threat. When the user identifies threats under "Other" SHRIMP guidance asks the user to consider consequences, but since there is no way to know what "Other" may be SHRIMP cannot assist by asking specific questions.

26. .1007 (c) If subdivision of system occurs, does the plan subdivide the system into regions with similar characteristics and for which similar actions are likely to be effective in reducing risk? Briefly describe the approach.

SHRIMP allows the user to subdivide the system anyway that makes sense. These include:

- *By material – SHRIMP requires users to subdivide by material when assessing external corrosion.*
- *By geographic regions*
- *By task(s) (for incorrect operations threat)*
- *By contactors or crews (for excavation threat)*
- *By type of equipment (for Equipment threats)*

The SHRIMP User's Guide includes a lengthy discussion of why and how to subdivide a distribution system.

27. (Information Only) Is the method used to evaluate and rank risks reasonable?

It is described in detail in an Attachment (11.3.2) to the Plan.

28. .1007(c) Are the results of the risk ranking supported by the risk evaluation model/method?

Yes

29. .1007(c) Did the operator validate the results generated by the risk evaluation model/method? Briefly describe.

SHRIMP asks the user to review SHRIMP's relative risk ranks and confirm that it is not at odds with the user's knowledge of the system. The risk ranking scores are displayed, along with a bulleted list of the factors that resulted in the risk scores. The SHRIMP User's Guide urges the user to consider other factors that were not included in the SHRIMP threat assessment process such as presence of schools, hospitals, etc. that would lead the user to move the threat higher in relative risk or factors that might lower the relative risk. The user may change the relative risk ranking, but must enter the reson in a text box, and that reason is written into the written DIMP plan.

30. .1007(c) Does the documentation provided by the operator demonstrate implementation of the element "Evaluate and Rank Risk"?

SHRIMP records all the major decisions made by the user and summarizes these in a Chapter of the written plan titled "RISK EVALUATION AND PRIORITIZATION."

31..1007 (d) Does the plan include procedures to identify when measures, beyond minimum code requirements specified outside of Part 192 Subpart P, are required to reduce risk?

For some threats a particular set of answers in the threat assessment results in the user being strongly urged to apply additional/accelerated actions to the threat. For external corrosion, an upward trend in corrosion leaks repaired, evidence of metal loss due to corrosion in exposed pipe inspection or failure to maintain CP criteria will trigger SHRIMP to suggest for A/A Actions.

For most threats, however, the SHRIMP Advisors were unable to define any objective criteria for establishing a relative risk level above which A/A Actions must be implemented, therefore SHRIMP defers to the judgment of the user whether the risk is high enough to warrant A/A Actions.

32..1007 (d) When measures, beyond minimum code requirements specified outside of Part 192 Subpart P, are required to reduce risk, does the plan identify the measures selected, how they will be implemented, and the risks they are addressing?

SHRIMP documents the measures selected and the threat they are addressing in Chapter 6 "ADDITIONAL/ACCELERATED MEASURES TO ADDRESS RISKS." The A/A Actions selected by the user and the threat are also listed in the attachment "Implementation Plan" which also includes information entered by the user explaining how the A/A Actions will be implemented.

33..1007 (d) Complete the table at the end of this form: Threat Addressed, Measure to Reduce Risk, and Performance Measure

34..1007 (d) Does the plan include an effective leak management program (unless all leaks are repaired when found)
   a. Locate the leaks in the distribution system;
   b. Evaluate the actual or potential hazards associated with these leaks;
   c. Act appropriately to mitigate these hazards;
   d. Keep records; and
   e. Self-assess to determine if additional actions are necessary to keep people and property safe.

SHRIMP offers the user three options:

- *Insert a cross reference to the user's existing leak management procedures.*
- *Adopt the GPTC Leak management guidelines.*
- *Insert text stating that all leaks will be repaired within 6 months, except for hazardous leaks that must be repaired or eliminated immediately. (This is the most stringent criteria in the GPTC guidance for non-hazardous, leaks and the SHRIMP Advisors felt it met the intent of "repaired when found.")*

The User's Guide cautions that states may have different requirements for leak management and the user should consult state regulations. Where state regulations go beyond GPTC, we anticipate that most systems will already have compliant leak management procedures and will use the cross reference option.

35. .1007(d) Does the documentation provided by the operator demonstrate implementation of the measures, required by Part 192 Subpart P, to reduce risk?

Implementation of the A/A Actions selected by the operator is outside of the scope of the written plan. Each operator must maintain records demonstrating that they are following through on the actions written into the DIMP plan.

36. Does the plan contain written procedures for how the operator established a baseline for each performance measure?

The section titled "e. Measure performance, monitor results and evaluate effectiveness" in Chapter 11.3 of the Plan describes how baselines for each performance measure are established. If a performance measure calls for data not previously recorded by the user, the results for 2011-12 will become the baseline.

37. Does the plan establish a baseline for each performance measure?

Yes, the user should describe what is the baseline for each performance measure in the Implementation Plan, Chapter 11.1

38. Does the operator have written procedures to collect the data for each performance measure?

The procedure for collecting data for each performance measure is included in the "Implementation Plan" attachment.11.1

39. Do the written procedures require the operator to monitor each performance measure?

If the user entered it in the Implementation Plan, yes – it will appear in Chapter 11.1.

40. .1007 (e) When measures are required to reduce risk, do the written procedures provide how their effectiveness will be measured?

Yes, in Chapter 7 "MEASURE PERFORMANCE, MONITOR RESULTS AND EVALUATE EFFECTIVENES" and also in the "Implementation Plan" attachment.

41. (Information Only) Can the performance measures identified by the operator in the plan be counted, monitored, and supported?

SHRIMP offers the user a choice of at least one performance measure for each threat, or the user may create its own. All SHRIMP-offered performance measure are quantifiable.

42. .1007(e) Does the documentation provided by the operator demonstrate implementation of the element "Measure Performance, Monitor Results, and Evaluate Effectiveness"?

Yes, in the Chapter titled "MEASURE PERFORMANCE, MONITOR RESULTS AND EVALUATE EFFECTIVENES"

43. .1007 (f) Do the written procedures for periodic review include:
    a. Frequency of review based on the complexity of the system and changes in factors affecting the risk of failure, not to exceed 5 years?
    b. Verification of general information (e.g. contact information, form names, action schedules, etc.)?
    c. Incorporate new system information?
    d. Re-evaluation of threats and risk?
    e. Review the frequency of the measures to reduce risk?
    f. Review the effectiveness of the measures to reduce risk?
    g. Modify the measures to reduce risk and refine/improve as needed (i.e. add new, modify existing, or eliminate if no longer needed)?
    h. Review performance measures, their effectiveness, and if they are not appropriate, refine/improve them?

The Chapter titled "PERIODIC EVALUATION AND IMPROVEMENT" includes a frequency of review chosen by the user not to exceed 5 years. It also includes other criteria that may trigger more frequent review.

In addition and enhancement under development will allow program re-evaluations to be guided and logged by SHRIMP. This will include verifying general information, incorporating new system information, re-evaluating threats and relative risk, reviewing effective of measures to reduce risk (through review of A/A Action-specific performance measures) and modifying the measures to reduce risk and/or performance measures as needed. We expect this to be available in May 2012.

44. (Information Only) Does the plan contain a process for informing the appropriate operating personnel of an update to the plan?

No. For most SHRIMP users this would be informing themselves. However SHRIMP has been modified to allow users to add their own text to any section of the SHRIMP plan.

45. (Information Only) Does the plan contain a process for informing the appropriate regulatory agency of a significant update to the plan?

Yes. An enhancement to SHRIMP currently underway will create a log in the current plan of all changes from the previous plan. This will be available for review during state agency inspection of the user. It does not automatically notify the agency that a significant revision has occurred.

46. .1007(f) Does the documentation provided by the operator demonstrate implementation of the element "Periodic Evaluation and Improvement"?

A log documenting that the user revisited all threat assessment, risk ranking and iother screens in SHRIMP to verify and/or update the information will be created by the SHRIMP program re-evaluation feature now under development. Documentation of a review of performance measures must be done by the user outside of SHRIMP, although keeping performance measures in SHRIMP is being considered for future product enhancements.

47. .1007(g) Does the plan contain or reference procedures for reporting, on an annual basis, the four measures listed in 192.1007(e)(1)(i) through (e)(1)(iv) to PHMSA as part of the annual report required by § 191.11 and the State regulatory authority?

Chapter 8 "PERIODIC EVALUATION AND IMPROVEMENT" includes procedures for reporting to PHMSA and states. For states the plan uses the address of the state agency provided to the SIF by NAPSR. If a state has a different address or means for receiving reports please provide it to the SIF and SHRIMP will be updated accordingly.

48. (Information Only) When required by the State, does the plan identify the specific report form, date, and location where it is to be submitted?

Only the address. See above. The SIF will include state report forms in SHRIMP if the states can provide that to the SIF.

49. .1007(g) Has the operator submitted the required reports?

SHRIMP cannot answer this question. The operator must submit any required forms and keep a record of doing it.

50. .1009 Does the operator have written procedures to collect the information necessary to comply with the reporting requirements of 192.1009?

Since each operator has unique recordkeeping systems and procedures SHRIMP cannot offer boilerplate text for this, however SHRIMP asks the user to describe the procedures for collecting this information and writes that into the attachment titled "Implementation Plan."

51. .1011 Does the operator have written procedures specifying which records demonstrating compliance with Subpart P will be maintained for at least 10 years?

The Recordkeeping chapter 10 of the SHRIMP written DIMP Plan states that the following records will be maintained for 10 years"

- *The current written DIMP plan,*
- *Copies of previous written DIMP Plans,*
- *Records of data required to be collected to calculate performance measures listed in Chapter 7, MEASURE PERFORMANCE, MONITOR RESULTS AND EVALUATE EFFECTIVENESS, and*
- *Records of mechanical fitting failures*

Because the SHRIMP written DIMP plan includes detailed descriptions of the answers provided to each question in the threat assessment process, the DIMP plan itself will contain a record of the design, construction, operation and maintenance data and decisions made by the operator in creating the written DIMP plan.

52..1011 Does the operator have written procedures specifying that copies of superseded integrity management plans will be maintained for at least 10 years?

Yes, in the Recordkeeping chapter 10 of the written plan.

53..1011 Has the operator maintained the required records?

That is up to the operator, although SHRIMP maintains copies of all current and superceded plans for 10 years.

For the top five highest ranked risks from the operator's risk ranking list the following:

- Primary threat category (corrosion, natural forces, excavation damage, other outside force damage, material or weld, equipment failure, incorrect operation, and other concerns);
- Threat subcategory (GPTC threat subcategories are acceptable. Try to be specific. Example, failing bonnet bolts of gate valve, manufacturer name, model #);
- Measure to reduce the risk (list the one measure the operator feels is most important to reducing the risk);
- Associated performance measure.