



PO Box 891993
Temecula, CA 92589
www.oursafetowns.com

24 January 2007

IP/CNPPD/Dennis Deziel
Mail Stop 8610
Department of Homeland Security
Washington, DC 20528-8610

SUBJ: *Comments on Chemical Facility Vulnerability Assessment Regulations RIN: 1601-AA41*

Mr. Deziel:

We have reviewed the proposed Chemical Facility Vulnerability Assessment regulations, and based upon our experience of implementing Risk Management Program/Process Safety Management Program Regulations for numerous facilities, regulating over 100 facilities required to comply with the California Accidental Release Prevention Program (the State version of the RMP regulations), assisting Sandia National Labs in developing their Chemical Facility Security Vulnerability methodology prior to their 2001 deadline, and performing Vulnerability Assessments on nearly 30 water facilities throughout the state of California, we have the following comments. Thank you for taking the time to review them, and if you have any questions, please do not hesitate to contact me. We have provided these comments in one of three categories: Regulatory, Business, or Methodology.

Very respectfully,

Stephen R. Melvin
President

Regulatory Comments:

- The Department has requested comments on appropriate sources to determine risk of a facility, how the "Top Screen" Process should work, and whether a Hazard Class approach would be the best solution. We suggest building a generic methodology that when a facility applies it, will tell them whether they are required to comply, but which most open source information would not reveal to an outsider. Similar to public key encryption, DHS promulgates the "public key" of what is required to comply, but the facility needs to have their "private key" of their information in order to determine if they are required to comply. Criteria might include: population possibly impacted by a release, potential impact to the country (in terms of a standard variable such as dollars) if the facility is damaged or destroyed, proximity to nearby targets of interest (stadia, universities, etc.), damage to a municipality's economy if the facility is damaged or destroyed, etc. While these are only a few, they need to be categorized in terms of variables that are applicable across the board (i.e. rather than measuring dollars of damage to a municipality's economy, one might measure percentage, or might measure both.) Each criteria would be "binned" to rank the facility within that criteria (e.g. if 100% of the locality's economy comes from a refinery, then that category might be ranked "5", whereas, if it is less than 5% of the economy, then it might be ranked "1".) If a facility is over a certain value in any category, or has an aggregate value over a certain amount, then they would have to comply.

While DHS would have to audit facilities to be sure that they completed the criteria correctly, they would not have to determine if the facility falls within the regulations. Since most of this information should be available to the facilities, it should be easy for them to comply, whereas DHS would have to locate the

information independently. Additionally, the Department would not have to “determine” if the facility was required to comply; the facility could determine that on their own and could get started complying without having to wait for the determination. This “advance notice” would allow the facility to take advantage of local economic conditions and work with local experts while not under as strict a deadline, thereby reducing the drain on local agencies and businesses all trying to assist the facilities to comply simultaneously.

- DHS requests comment on whether a facility can compel facilities that have not been deemed “high risk” facilities to complete a “Top Screen” process. The answer is yes. While the law requires risk-based regulations, there is no requirement that only high-risk facilities have to take action. Even low- and medium- risk facilities should be aware of where they stand in terms of their plans and vulnerability. The EPA's general duty clause under the Risk Management Program made this fact abundantly clear.

- DHS requests comments on the “Top Screen” process and which facilities should be required to complete the process. Specifically, addressing the question of whether RMP facilities should have to complete the process, it is unclear whether this requirement would apply to facilities that meet the threshold quantities for the RMP regulations, but fall under the “flammable fuels exemption” that was later passed. Additionally, we feel that it is impractical to expect facilities to comply with the requirements of the proposed rule with the Top-Screen criteria being classified as security sensitive information. See the comment above on business compliance.

- DHS has requested comment on the following specifics:

1. How many risk based tiers should DHS create? Three to Four. More would be confusing, less would not provide enough granularity.
2. What should be the criteria for differentiating among the tiers? See the above recommended methodology.
3. What types of risk should be most critical in the tiering? Considering that all of the information discussed is facility based rather than community based, the highest priority should be given to “public impacts” (number of people who could be killed in a public way, i.e. at the Superbowl), followed by “private impacts” (number of people who would be killed in a less public way, i.e. in their homes), followed by economic impacts, followed by all other impacts.
4. How should performance standards differ among risk-based tiers? It is unclear from the regulations how the performance standards will be measured, so this question is difficult to answer. For example, the performance standards discuss “securing the perimeter” of the facility, but don't discuss who or what the perimeter will be secured against. Securing a perimeter against a single adversary with fence cutters is a different task altogether from securing it against an armed assault team with automatic weapons and explosives.
5. What additional levels of regulatory scrutiny should apply to each tier? There should be no additional scrutiny applied to each tier, although obviously, there will be more scrutiny required during the reviews for the more complicated tiers. Consider delegation to local and state authorities (similar to that allowed under the RMP regulations) to allow the local regulators (that are already working with the facilities and performing inspections) to maintain the relationships they already have and allow for more hands-on regulation than DHS could provide.

- DHS should consider defining nationwide risk standards. While the risk matrix provided in Appendix B (the RAMCAP methodology) is suggested, it is not required. The result will be a hodge-podge of risk matrices used throughout the country, meaning that one facility cannot be compared to another facility and thereby reducing DHS' ability to determine where best to focus their attention.

- DHS states that the regulations need to require facilities to “...appropriately address the Vulnerability Assessment and risk-based performance standard for security for the facility.” In Section 27.225, DHS requires the facilities to develop a Site Security Plan to meet the standards laid out: (2)

“...potential modes of terrorist attack...” and (3) “...how security measures ... will address each ... performance standard...” At no time in the regulations however, does DHS specify what is an acceptable risk level, or how to measure the performance standard. It is impossible for a facility to comply with the regulation if they don't know what the end state is. Also, facilities need to know if it is possible for them to reduce their risk so that they can move to the next lower tier, or if bringing in a new chemical or increasing the quantity of an existing chemical will result in them being moved into a higher-risk level.

- The proposed regulations mention that the Department is considering accepting other methodologies as certified by the Center for Chemical Process Safety (CCPS). If DHS makes this blanket judgment, then the Department should also consider accepting methodologies certified by the American Petroleum Institute (API) or by Sandia National Labs as equivalent to their methodologies. Especially since the Sandia methodology was developed for the US Department of Justice specifically to determine the vulnerability of Chemical Facilities nationwide, this methodology should at the least be considered.

- The proposed regulations state: “a Site Security Plan must address both the “Vulnerability Assessment” for the covered facility and the applicable “risk-based performance standards.” Since the VA should be written to address the applicable “risk-based performance standards”, this statement is redundant.

- The proposed regulations state that the performance standards will require covered facilities to explain how they will a) secure and monitor the perimeter of the facility, and b) secure and monitor restricted areas or potential targets within the facility. (Section 27.230(a)(1) and (2)) If the perimeter is secured, then there is no need to further secure the internal areas except against insiders or insider collusion. This difference should be brought out in the proposed regulations. Also on this point, it is unclear from the proposed regulations what the perimeter needs to be secured against. As previously mentioned, it takes more resources to secure a perimeter against an assault team with automatic weapons than against a single intruder with a belt-bomb. A vehicle borne explosive device may be even more difficult to protect against as it may not even have to breach the perimeter. Lastly, an example of a perimeter that may not be securable is a farm which used ammonia or ammonium nitrate to fertilize crops. While either may be on the list, and in fact, there have been ammonia releases due to valves being left open after theft, securing the entire perimeter of the farm may not be a practical option.

- The proposed regulations seem to overlap with HM222 by requiring that the facility secure and monitor the shipping and receipt of HazMats (Section 27.230(a)(5)). Additionally, it is unclear at what point the HazMat becomes the shipper's responsibility vice the facility's responsibility. This delineation of responsibilities is critical to allow businesses to properly comply with both sets of regulations.

- The emergency plan calls for responding to security events internally, but not immediately adjacent to the perimeter. All security events that can affect the facility should be addressed by the emergency plan.

- The proposed regulations call for background checks on personnel and visitors, but not for vendors. Vendors need to be screened as diligently as any employees since they have almost as much access, but much less regular scrutiny in many facilities. Background checks will be expensive and time consuming if the government conducts them however, it will be necessary to set standards for what should be investigated in a background check if private industry will be conducting them.

- DHS also requests comments on whether workers should be required to participate in a program similar to the Transportation Worker Identification Credential program. If such a program is instituted, it will be necessary to allow sufficient time for implementation. Otherwise, the facilities may be shut down by the loss of trained workers who are not credentialed. Additionally, while this comment should not prohibit the implementation of such a program, this type of program may “force” the hand of any sleeper terrorists causing them to attempt an attack prior to the facility having the rest of the program in place. As a result, such a program should be implemented last in the succession of security measures.

- It is unclear from the regulations how the facility will report significant security events to DHS,

even though such reporting is required. It is also unclear what method will be used to provide the VA or Site Security Plans to DHS. Is electronic submittal acceptable? If not, what couriers will be acceptable to DHS? What is the address for mailing? These items should be addressed in either the regulations or in an associated fact sheet provided simultaneously with or shortly after the regulations are finalized.

- There is no definition for “adequate” or “appropriate” records (Section 27.230(a)(18), although the proposed regulations call for the facility to keep them. What is “adequate” or “appropriate”? Section 27.250 sets out recordkeeping requirements, but there are still many questions. For example, while the requirements for the training records are specified, there is no list of what training is required. Descriptions of incidents are required, but the level of incidents is not specified. Audit letters are specified, but since audits are not required by the facility, it is unclear if a letter is required when a facility conducts an internal audit.

- DHS seeks comment on the proposed system for review and approval. Under Section 27.220(b)(2) and (3), the Assistant Secretary may extend applicable deadlines pending resolution of an objection. The regulations should stipulate a) how long the Department has to respond to an objection and b) ensure that the facility's deadline is placed in abeyance until the objection and all appeals are denied.

- DHS states that the DHS website will have guidance for submissions requesting approval for existing security plans. Even though the Department was accepting submissions by Dec 28, 2006, as of Jan 23, 2007, we were unable to find the guidance document on the website.

- We do not think that an immediate inspection upon receipt of additional threat information will enhance the security of the facility. These programs will take time and resources to set up, and a surprise inspection will not assist the placement or creation of these programs unless DHS plans to bring additional resources and/or funding to assist the facility in setting up their programs, installing new equipment, etc.

- The proposed regulations state that DHS will approve or disapprove each VA, but not whether they will approve or disapprove any updates or changes. E.g. VAs were required for water departments, but there are no requirements for updates to those plans.

- DHS states that tier one facilities will have to submit VAs to the Department within 60 days. The regulations are unclear as to whether this is 60 days from the finalization of the interim regulations or 60 days from notification by DHS.

- DHS requests comment on the categorization of sensitive information. We believe that it is acceptable the way it is laid out in the proposed regulations.

- We have no comment on the applicability of this rule to facilities covered by the Maritime Security Transportation Act of 2002.

- DHS requests comments on whether Ammonium Nitrate facilities should be treated differently than other facilities. We believe that they should be treated no differently than other facilities, although the presence of Ammonium Nitrate should be a factor in the Top Screen process.

- DHS has the ability to determine that a facility does not present a high level of security risk and will issue a notice to the facility to that effect. How does DHS plan to ensure that these facilities do not later change their chemicals or processes and so become a facility that presents a high level of security risk?

- DHS requests comments on the requirements that the submitter of the facility be an officer of the corporation, be domiciled in the US, and be a citizen of the US. We agree with these requirements as it will ensure that the officers of the corporation understand their commitments to the government.

Business Comments:

- If the requirements are less stringent for lower tiers, then there is no reason why the lower tiers should not have to update at the same pace as the higher tiers. Currently, the pace is different and also out of sync with other regulations that facilities currently have to comply with. Suggest changing the cycle so that updates are due on the same schedule as RMP/PSM audits to ease the burden on industry, or if there are significant changes to the site, process, chemicals, or specific threat to the industry.
- The proposed regulations state that DHS may audit facilities themselves, or may certify third party auditors to perform the audits. It is unclear whether these third party auditors will be hired by DHS, or by the facility.
- The proposed regulations call for the proper training, exercises, and drills of facility personnel. It is unclear that this includes all facility personnel as opposed to just security personnel and many facilities will interpret the regulations the former unless all personnel are called out in the regulations.
- DHS will allow facilities that have not been selected as high-criteria to voluntarily submit to the screening process. Our experience is that most facilities, unless they are required to do so, will not participate in the process.
- DHS believes that these regulations can be revised any time after the initial proposed regs are finalized. DHS needs to set a limit on how often and when these regs will be revised so that business can comply without trying to constantly trying to hit a moving target.
- There is currently no solid criteria to determine whether a facility is required to comply with part or all of these regulations. DHS has reserved the right to declare that a facility is covered based on an evaluation of the “Top-Screen Material” provided by the facility. Again, businesses are trying to hit a moving target. In general, businesses want to comply with the law but need to be able to plan their budgets and operational cycles based on regulations and these amorphous criteria don't allow businesses to properly plan. The information of whether a facility is in or out is currently determined to be security sensitive information. While releasing this information may increase the likelihood that a terrorist would be able to use it as a targeting mechanism, keeping it security sensitive will certainly make it more difficult for businesses to comply and will increase regulatory overhead tremendously.
- 60 days to complete a Vulnerability Assessment and develop a site security plan which addresses the risk-based criteria as set forth in the proposed regulations is sufficient time only if a facility already has the resources. If they do not, they will need to train their personnel on the RAMCAP methodology (or other approved methodology), or hire a consultant who is familiar with the methodology which will take time – especially if many facilities in a geographic area are required to submit simultaneously, as most consultants can only supply the needs of a few facilities. The result may be that some facilities will not have the expertise necessary to conduct a good assessment, resulting in poor data to DHS. Note also that required information includes: chemical names, nature, conditions of storage, etc. For a large facility, collecting this information in a single place may take weeks if they have not already done so to comply with other regulations. Lastly, note that a similar law (the Bioterrorism Act of 2002) required Vulnerability Assessments from large water agencies, but gave them 180 days to comply. While still difficult, this is a much more realistic timeline than 60 days.
- There are circumstances under which DHS might issue a cease operation order. Note that such an order may not make the facility any safer, and may in fact increase its risk. The chemicals will still be onsite, but there may be fewer personnel who can help prevent problems if there is a safety or security event. While these orders might be necessary, note that they are most likely punitive only.
- We have no comments on the appeals and objections process, with the exception that they look to be very time consuming to DHS and we would hope that sufficient technical manpower would be available to address these issues without taking away technical resources from working with facilities to make themselves safer.
- Note that if DHS is the only agency sponsoring technical assistance, and they decide to contract

out the specific technical assistance provided to facilities, then it is quite possible, given the short time frame of the regulations, that a single company will get the contract. While this is not a problem from a contracting point of view, it does mean that the company receiving the contract will very likely be providing their personnel who may have no experience conducting Vulnerability Assessments (but have completed a “methodology class”) to train facilities while smaller technical experts in the field may not be called on to assist in providing this training to facilities. In other words, when fighting terrorists, DHS should be using every available resource, and not choosing the easy path of a single contractor who may or may not be able to provide the best technical information to facilities.

- DHS requests comments on the economic impact of the rules on facility owners/operators. The costs will be significant. They can be minimized by aligning these security regulation with regulations with which facilities are already complying such as RMP and PSM. This combination includes not only the requirements for whether the facilities must comply or not, but also the requirements of update and submission cycles, reviews, and if possible, finding a way to combine inspections and audits.

- DHS also requests comments on the benefits of the rulemaking. We see two major benefits to these rules. First, many facilities that have been waiting for the regulations to develop their Vulnerability Assessments will be spurred to take action and will develop their programs. Second, there is an opportunity with these regulations to actually standardize the programs across the country (allowing for location, threat and community differences.) DHS can capitalize upon this opportunity by ensuring that the risk-based standards have common risk matrices, with similar definitions of severity and likelihood. Additionally, DHS can ensure that facilities are required to develop their Site Security Plan to the same standards: i.e. by defining what risk is acceptable for a given scenario, by providing realistic and common probabilities of attack, and by providing guidance to marry this methodology with those used in facilities' safety programs.

- DHS requests comments on the economic impacts to smaller communities. Note that many facilities will be speaking with their local regulators to determine the best ways to coordinate and comply with these regulations. We understand that DHS intends to provide technical support to the facilities, but the relationships that many have already forged, coupled with the requirements to coordinate emergency response to security events with local responders, will mean that they will be contacting their local agencies. While all municipalities will have an additional burden placed upon them to assist facilities in complying with these regulations, smaller cities will especially have a difficult time assisting businesses in complying with them.

- While DHS intends to draw on several other regulations in order to find all of the facilities required to comply with this regulation, it is unclear how they intend to get the names, addresses and contact information for each of these facilities. For example, the Risk Management Plan regulations and Process Safety Management regulations “push” the requirements out to the facilities. In other words, if they have over a certain threshold quantity of chemicals, they are required to comply with the regulations. Since DHS intends to notify each facility of their status after completing the top-screen process, it is quite possible that many facilities will not complete the top-screen process, because they will not realize that they are required to do so.

Also, while the regulations specify that DHS will make the determination after a facility completes the Top-Screen process, the regulations do not specify a timeframe for DHS to make that determination following submission of the material. In order for a business to properly plan their business practices to comply with these regulations, they need to be able to plan, and knowing when they will have their determination after completion of the process is critical.

- The listed definitions include the “Owner” of a facility. It is unclear from the definition if a landlord who rents space for a facility would be responsible for complying with these regulations or if the operator would bear that responsibility.

- DHS should provide a method by which facilities can remove or reduce quantities of chemicals and reduce their risk sufficient to remove them from the program or lower their tier.

- Section 27.230(a)(9) requires that the facility develop their plan with the assistance of local law enforcement and first responders, but does not address the implications if those agencies do not have the resources to properly assist the facility in developing their plan. This section also requires that the facility maintain effective monitoring, communications and warning systems, but again, does not specify what they need to be effective against, and does not specify how effective they need to be. For example, do the facilities need to hire a “red team” to try to stage a break-in to their facility, or is a tabletop and annual testing of the equipment sufficient?
- Section 27.230(a)(15) requires that the facility report “significant” security incidents to the Department, but does not define what a “significant” event is. Without formal training, most facilities would not recognize that the “vagrant” sitting across the street at the bus stop is a potential adversary. There is also no requirement to communicate with similar facilities in the local area (through Local Emergency Planning Committees, Business Advisory Groups, Community Awareness and Emergency Response groups, etc.) We suggest setting up working groups through Terrorism Early Warning Groups (such as the Orange County Private Sector Terrorism Response Group) specifically designed to address chemical incidents and look for local patterns.
- Section 27.245(a) allows third party auditors for facilities that are not in the higher-risk tiers, but it is unclear why the higher-risk tiers are exempted from this. If DHS trusts the auditors, then they should be acceptable even at the higher-risk tiers. If DHS does not, then they should not be acceptable at the lower tiers. Additionally, the regulations allow less flexibility to DHS to address the needs of the facilities, especially if resources become scarce.

Methodology Comments:

- Note that Section 27.215(a)(3), when describing Vulnerability Assessments, does not mention scenarios, but instead leans heavily in the direction of asset-based studies.
- Under Sections 27.215(c) and 27.225(b)(2), the regulations discuss updates and revisions, but only specify that they are required if requested by DHS or on a schedule to be published later. This is impractical because DHS will not know if the facility changes their process or chemicals. Suggest incorporating an aspect of the RMP and PSM regulations: Management of Change (MOC), which requires updates in the event of a significant change to the facility or process. Note also that 27.215(c)(3) requires notification to the Department upon any changes to the VA, but this presupposes that the facility will revise their VA if the process or facility changes – which is not required by the regulations.
- DHS has asked for comments about “grouping” facilities into “model facilities.” This methodology will only work if each “model” is truly an accurate model of the facility. For example: a farm that uses anhydrous ammonia could be 30 acres or 300 acres. A facility that uses cyanide as part of its plating solutions may be in a warehouse, attached to other facilities in an industrial complex, or not even in town. A petroleum refinery can range from a 10 unit refinery that produces some fuel, but also uses the heavier carbon chains to produce asphalt to a 40 unit refinery with sulfur dioxide to make sulfuric acid, a 6 story tall Coker, and a hydrocracker. On the other hand, it is not practical to group facilities by size as they may have completely different processes.
- DHS asks if risk-based criteria should be used in the “model facility” criteria. We believe that it should. DHS also asks if size should be a factor. While it might be a factor, beware putting too much emphasis on it. A single tank farm with a single chemical may span a much larger area than a plating shop with numerous chemicals and processes. Also in this category, DHS asks if facilities that might be targeted for theft should be treated as a separate category for modeling purposes. We do not believe so. We think that the costs involved in protecting such a facility will likely be on the order of magnitude as those for other facilities. Lastly, note that the enhancements listed within the proposed regulations (for which costing data will be used to categorize model facilities) do not include procedural changes, or buffer zone issues – both of which could be significant in terms of cost to a facility.

- DHS suggests that the Top-Screen criteria include "...the potential loss of the capability to execute a critical mission...", but it is unclear if that critical mission is the facility's mission, the city's mission, or other mission. Additionally, if DHS provides a list of chemicals as part of the Top Screen process, DHS should be certain to distinguish between anhydrous and aqueous ammonia as they have the same CAS number and failure to distinguish between them has caused much confusion with safety regulations.

- We do not understand the disparity in damage between flammable and toxic chemicals. If a flammable chemical is dangerous when it exposes 1000 people, then a toxic chemical should also be dangerous at that threshold.

- The proposed regulations use damage to "key transportation assets" as a screening factor, but they do not define "key transportation assets." Additionally, the screening process does not appear to address other transient populations such as amusement parks or stadia. In addition to addressing this in the Top Screen process, we suggest changing the last paragraph in Section 1.5 of the methodology to read: "Proximity to off-site population and other off-site targets..." to address this discrepancy.

- While we do not inherently disagree with the 35% threshold for US Domestic Production Capacity or DOD market share, we are unclear as to the methodology that determined that number. 35% seems incredibly high for critical chemicals or for warfighting capability, and a lower percentage might be more beneficial when determining true impacts.

- The proposed methodology states that each infrastructure will use the same threats. While this methodology makes it easy to compare one infrastructure to another in terms of threats, the consequences will be different for each infrastructure, and so comparing the results seems to be comparing "apples to oranges." A contamination threat to a chemical facility has much different results than a contamination threat to a water facility or a food processing plant, and it makes no sense at all to look at the effects of contaminating a National Monument, except as a WMD event.

- The methodology states that the facility would not be "expected to prevent or protect against the scenario." Note that the regulations themselves state that the facility needs to develop a Site Security Plan to meet the standards laid out. (Section 27.225) These two statements seem inconsistent.

- During Step 2 of the RAMCAP methodology, DHS provides the threats at a sector level. Note that the chemical sector is differentiated by location and by process. For example, a chemical refinery in rural Colorado may have a different set of threats in Los Angeles, and they would both have different threats than a chlorine processing plant, or an ammonia refrigeration facility.

- During Step 3 of the RAMCAP methodology, DHS discusses the ability to perform the study as either an "asset-based" study or as a "scenario-based" study. Note that while most of the methodology pays lip service to a "scenario" based approach, the methodology as laid out is heavily geared towards "assets" as can be shown by reading the glossary where most of the definitions are geared toward "assets" (see "capability" for an example.)

While a good facilitator can achieve the objectives of a Vulnerability Assessment using any methodology, our experience is that by using a methodology that focuses on "assets", most untrained or semi-experienced individuals will lose sight of smaller causes that could have significant impacts. For example, while the "asset" might be a tank which the adversary might desire to overflow, the team may focus on all of the causes in the immediate vicinity of the tank, neglecting a pump that is located hundreds of feet from the tank and with several intervening pieces of equipment. As a result, an "asset" based approach requires a much greater level of skill and experience to obtain complete results, thereby causing an increase in costs for the facilities when conducting these studies.

One question that should be clarified in either guidance or in the regulations themselves is whether a scenario-based approach can be conducted as part of a Process Hazard Analysis (PHA) or Hazard Review (HR). If so, are there methodologies that will be unacceptable for such inclusion? (e.g. What-If, What-If/Checklist, Checklist, HAZOP, FMEA, TRIZ, etc.)

- During the planning phase of the methodology, DHS states that "The team should be

knowledgeable of and experienced at the process they are reviewing”, and that “The team leader should be knowledgeable of and experienced in the VA process methodology.” The RMP and PSM processes specify the minimum requirements of a team (operations experience, understanding of engineering, experience in the methodology.) and the VA regulations should specify the minimum requirements for a VA team (e.g. There is currently no security experience required, although it is listed as a typical member.)

Under “Locating Required Data”, the following data should also be available to the team:

1. Fire Response Plans
2. Risk Management Plans
3. Process Safety Information/Plans
4. Standard Operating Procedures
5. Historical Accident Data

Additionally, P&IDs should read Piping and Instrumentation Diagrams; and LEPC stands for Local Emergency Planning Committee.

- Under “Data Collection and Review”, instead of “the operator” flagging the absence of information, it should be “team members.”
- Under “Analyzing Previous Incidents Data”, historical accident data should be included, as this data could help the team understand the consequences of events.
- In Figure 6, 1.1 refers to critical assets, but doesn't define “critical.” 1.2 refers to assets that support “critical” functions. Again, “critical” is not defined, and it is unclear if these assets are the same as the assets from 1.1. Section 1.3 discusses “critical” operations of each asset, but does not specify if these assets are from 1.1, 1.2, or both. Section 1.5 specifies “hazards and consequences or impacts to the assets and critical functions”; it should refer to all hazards, consequences, and impacts. This is an example of an asset based approach missing items that a scenario based approach would not.
- Note that in Step 1.5, the methodology refers to using the EPA RMP offsite consequence analysis as a starting point for determining the consequences of toxic or flammable releases. Since some of the chemicals for which DHS may be requiring VAs may not fall under the RMP regulations, this comment may not apply. Also note that the implication from this statement is that only RMP chemicals will be regulated by DHS.
- DHS states that “asset owners may consider using a matrix such as [the one provided]” however, as mentioned earlier, the information needs to be consistent from facility to facility in order to compare one to the other. As an example, while DHS suggests that business interruption might be a factor to consider, the loss of \$10,000/day may be a low to moderate impact for a major refinery, but may be classified as a major impact for a minor food processing plant that uses ammonia refrigeration.
- The RAMCAP methodology currently ranks items from 1-5 where 5 is high and 1 is low. The potential long-term impacts of this ranking style are best shown by a severity example. If 5 is high, and a facility counts it as one death, then the question arises, “What about 10 deaths, or a hundred?” Eventually, someone adds a 6 to the scale to be worse than the 5. Then the next step is adding a 7 for the loss of the entire facility and all of the people. If this facility sets off another facility and both facilities are lost, then someone adds an 8 to be worse. Eventually, the loss of a single life as the original “worst case” is lost. By setting the highest scale as 1, there is a standard past which the facility does not go and the meaning of “worst case” remains constant. This is important both for comparing to other facilities and for historical comparison. An example is the Safety Risk Scale that many facilities use of a single death as their highest severity, whereas the suggested consequence categories for the RAMCAP methodology show up to 100 deaths as the lowest category of severity. Similarly, the “Completing the Worksheet” step, Item 7 refers to a consequence scale of 1-5, although the figure shows 1-10.

- The RAMCAP methodology sidesteps the question of likelihood by suggesting that facilities assume that international terrorism is possible at every facility. This approach does a grave disservice to the facilities and skews the results of the studies to show an abnormally high likelihood of these events. While comparison to safety events is not practical (orders of magnitude difference), there are at least comparative methodologies for demonstrating the relative likelihoods between facilities in different localities and processes or between different adversaries such as international and domestic terrorists. One approach is for DHS to define a baseline facility and assign relative likelihoods to events based upon the “model approach” described earlier so that facilities can at least understand the relative impacts of their Site Security plans rather than developing them in a vacuum.

- Step 3.3 refers to “...the subsequent destruction or theft of an asset.” We suggest rewording this to read “...cause an event or steal an asset.”

- We suggest rewording Step 3.3, Item 2, from “Causing the deliberate loss of containment of a chemical present at the facility” to “Causing a release of a chemical present at the facility to impact workers or the public.”

- The “Completing the Worksheet” step, Item 8 discusses existing countermeasures but fails to address mitigating countermeasures, relying instead solely on security countermeasures.

- Note that Item 11, Likelihood: describes a process of assigning a likelihood value that is inconsistent with the methodology earlier proposed of assuming that an attack is possible at all facilities. See the earlier discussion of relative likelihoods.

- In Step 4: Risk Analysis/Ranking, the methodology proposes a High, Medium, and Low ranking. Note that if a facility uses a software program to track this data, the scenarios will automatically be sorted High, Low, Medium as the programs sort alphabetically. We suggest using a 1,2,3 scale instead, where 1 is High Risk and 3 is Low Risk.

- In Step 3.7, Identify Countermeasures, the methodology states that “...the team should ensure each scenario has the following countermeasures...” The team should instead restrict this to high and moderate risk scenarios, vice having to plan countermeasures for low risk scenarios. Later in the same section, the methodology states that: “The team attempts to lower the the risk to the corporate standard.” At no other time do the regulations or the methodology refer to a “corporate standard”, explain how to develop one, or who is responsible for it. We suggest deleting this line, modifying it to remove the reference, or defining the standard and providing guidance on it.

- In the “Follow-up to the VA” section, the outcome of the VA is to “...reduce risk to an acceptable level.” We suggest clarifying whether DHS or the facility determines what is acceptable.

- In the Glossary of terms, we have the following recommendations:

Adversary: Any individual, group organization, or government that conducts activities, or has the intention and capability to cause damage, business interruption, espionage, or injury/loss of life. (etc.)

Asset: modify “owner” to “owner/operator”.

Countermeasures: include mitigating countermeasures.

Likelihood of Adversary success: this term is not actually used in the methodology as written.

Process Hazard Review (PHA) – this definition can also be applied to Hazard Review (HR).

Risk Assessment – the letters “R” for Risk, “V” for Vulnerability, “C” for Consequences, and “T” for Likelihood are not used in the document until the glossary. The document should be consistent.

[Add] **Collusion/Colluding Threat:** An external threat working together with an internal threat.