

# Appendix 3: The Protection Program

## Appendix 3A: NIPP Baseline Criteria for Assessment Methodologies

The purpose of this appendix is to specify the baseline criteria for methodologies used to support all levels of comparative risk analysis under the NIPP framework. Many owners and operators have performed vulnerability and/or risk assessments on the assets, systems, and networks under their control. To take advantage of these activities, DHS and the SSAs will use the results from previously performed assessments wherever possible. However, the assessment work to date has varied widely both within and across sectors in terms of its assumptions, comprehensiveness, objectivity, inclusion of threat and consequence considerations, physical and cyber dependencies, and other characteristics. In order to use previous assessment results to support national comparative risk analysis, the methodologies used to perform the assessments must be tested against the NIPP baseline criteria.

### 3A.1 Baseline Criteria

There are seven criteria that constitute the national baseline, categorized generally into two different groups. The first group tests the methodology to ensure that it will be credible to objective users of the analysis produced by methodology; the second group tests the methodology to ensure that it will be comparable with other standard methods used in comparative sector or national risk assessment.

To be credible, a methodology must have a sound basis (it must have integrity); it also must be complete and the analytic method and associated assumptions must be defensible. These factors are reflected in the first three elements of the criteria. To be comparable, the methodology must be documented, transparent, reproducible, and accurate; these factors are reflected in the last four elements of the criteria.

The following questions provide a simple way to determine which aspects of a methodology meet the baseline criteria. The questions also provide a guide for improving the methodologies or changing them so that they can meet the baseline criteria. A methodology meets the requirements of the baseline criteria when all of the questions can be answered in the affirmative.

### Is the Methodology Credible?

1. **Integrity (sound basis):** Is the methodology based on documented risk analysis and security vulnerability analysis? Does it specifically address:
  - a. Consequences?
  - b. Vulnerability?
  - c. Threat?
2. **Complete:** Does the methodology provide reasonably complete results via a quantitative, systematic, and rigorous process that:
  - a. Provides numerical values for estimated consequences, vulnerability, and threat whenever possible, or uses scales when numerical values are not practical?
  - b. Specifically addresses both public health and safety and direct economic consequences?
  - c. Considers existing protective measures and their effects on vulnerabilities as a baseline?
  - d. Examines physical, cyber, and human vulnerabilities?
  - e. Applies the worst-reasonable-case standard when assessing consequences and choosing threat scenarios?
  - f. Uses threat-based vulnerability assessments?
3. **Defensible:** Is the methodology thorough and does it use the recognized methods of the professional disciplines relevant to the analysis? Does it adequately address the relevant concerns of government, the CI/KR workforce, and the public?

### Is the Methodology Comparable to Other Methodologies?

1. **Documented:** Does the methodology provide clear and sufficient documentation of the analysis process and the products that result from its use?
2. **Transparent:** Is the methodology easily understandable to others as to:
  - a. Assumptions used?
  - b. Key definitions?
  - c. Units of measurement?
  - d. How it is to be accomplished?
  - e. Basis for expert judgments and risk decisions?
3. **Reproducible:** Does the methodology provide results that are reproducible or verifiable by equivalently experienced or knowledgeable personnel?
4. **Accurate:** Is the methodology free from significant errors or omissions so that the results are suitable to inform decisionmaking?

Given the unique nature of the individual CI/KR sectors and the assets, systems, and networks that comprise them, details of the baseline criteria must be tailored to each sector. DHS will work with the SSAs and other sector security partners to accomplish this tailoring; however, the baseline criteria above are generally applicable to each sector.

Existing assessments or methodologies will be considered by DHS as meeting the NIPP Baseline Criteria and, therefore, are suitable for national and sector-level comparative risk analysis if they can provide an affirmative response to the questions above. Assessment or methodology evaluations will be done in coordination with the SSA, SCC, and GCC, as appropriate.

## 3A.2 Specific Aspects of the NIPP Baseline Criteria

**Based on classical risk analysis.** As outlined in chapter 3 of the NIPP, risk analysis consists of three primary elements: consequence, vulnerability, and threat. To be considered credible, a proposed methodology must include all three components of risk.

**Provide numerical values when possible; use scales when necessary.** Risk typically can be measured either quantitatively (i.e., numerically) or qualitatively (i.e., descriptively). Public health and safety and economic impacts generally lend themselves to quantitative measurement (e.g., number of lives lost, cost in dollars of rebuilding or restoring an asset), whereas psychological and governance impacts are often measured qualitatively. For quantitatively measured consequences and their associated risk, accurate numerical estimates should be used whenever possible. When it is not practical to use such estimates, scales should be used to reflect the assessed outcome using either numerical ranges (for quantitative metrics) or detailed descriptions (for qualitative metrics). The use of numerical ranges and/or detailed descriptions is necessary because terms such as “low” or “high” are subject to varied interpretation by different users. DHS will provide sample ranges and descriptive language to security partners, and will work with them to establish “translators” that facilitate the conversion of results using other methodologies to standard scales to support national comparative risk analysis.

**Consider human and direct economic consequences.** For the national comparative risk analysis conducted by DHS, the consequences of interest are those of national significance as established in HSPD-7. These consequences can be divided into four main categories: human, economic, public confidence, and government capability. Because accurately estimating consequences other than direct injury, loss of life, and economic effects is complex and often beyond the scope of an individual owner/operator’s expertise, this element of the baseline criteria requires assessment methodologies to address the following two types of impact at a minimum:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries).
- **Economic Impact:** Direct effects on the national, State, tribal, or local economy (e.g., cost to rebuild facility, system, or network; cost to respond to and recover from attack; other clearly definable incident costs resulting from unavailability of product or service; or long-term costs due to environmental damage).

**Consider existing protective measures and their impacts as the baseline.** In evaluating the extent to which an asset, system, or network is vulnerable or an attack is likely, an assessment should consider the existing measures that are in place to reduce that asset, system, or network’s exposure to the relevant threat scenarios. Specifically, security specialists should examine the ability of an asset, system, or network’s existing security profile to deter, detect, devalue, defend against, mitigate, respond to, and recover from the most relevant threat scenarios.

**Use worst-reasonable-case standard.** Risk assessments are significantly influenced by the estimated or assumed level of success or severity of a given threat scenario (e.g., worst case, worst reasonable case, most likely). For the purposes of national comparative risk assessment, methodologies should use a worst-reasonable-case scenario.

**Examine physical, cyber, and human vulnerabilities.** When evaluating risk, many vulnerability assessments focus solely on physical security; however, physical security is only one aspect of a robust vulnerability assessment. Vulnerability assessments should also assess personnel security and other human security issues, cyber security and network architecture issues, operational security, and infrastructure dependencies and interdependencies.

**Scenario-based vulnerability assessments.** The suite of tools that DHS is developing and using for vulnerability assessments is scenario based, meaning that the assessments measure the susceptibility of an identified asset, system, or network to a specific threat scenario (e.g., successful detonation of a nuclear bomb, successful detonation of a car bomb, etc.). This allows the assessment to be informed in general terms by potential adversary tactics and attack vectors. Consequently, vulnerability assessment methodologies used to support cross-sector comparative risk analyses should be scenario based, and certain

specific scenarios or their equivalent should be used. In light of the distinct characteristics associated with different types of assets, systems, or networks, DHS will work with sector partners to identify which threat scenarios are most appropriate in the context of the sector-specific landscape.

**Defensible on logical grounds.** In order to produce analysis that is credible to those who must use its results, a methodology must adhere to the recognized methods of the professional disciplines that are relevant to the method of analysis (e.g., economics, engineering, medical profession), and it must reasonably and adequately address the concerns raised by the three groups who may be directly affected by the decisions based on its results: (1) governments at all levels, (2) the CI/KR workforce, and (3) the public at large.

**Documentation is necessary to enable comparison with other methodologies in use.** Written documentation that is clear and sufficiently complete to allow a comparison of strengths and weaknesses with respect to other methodologies used in the national comparative risk assessment is necessary. This should include a description of assumptions, definitions, units of measurement, time horizon, the general order and steps of the assessment, calculations, and the basis for any expert judgments that the methodology relies on that are not readily apparent.

**Need to be easily understandable.** In addition to the existence of written documentation, a methodology must be easily understandable to others with appropriate knowledge and experience. This means that:

- Assumptions must be stated;
- Key definitions must be provided;
- Units of measurement must be specified;
- Analytic process by which the methodology is executed must be specified; and
- Basis for expert judgments used in lieu of explicit calculations or analysis must be provided.

**As with any deliberate process, the results of applying the methodology must be reproducible or verifiable by others of requisite knowledge and experience levels.** The methodology must be sufficiently defined and deliberate so that any qualified person could replicate the results it produces; it must not depend on hidden judgments or opinions.

**Must be free from logical errors of omission or commission.** Because the results of risk assessments will be used to inform decisions regarding homeland security, the accuracy of the methodology must meet a high standard. While estimates and approximations often must be used, the tradeoff between practicality and accuracy must be carefully taken into account and, in no case, should logical or mathematical errors be accepted.