1 November 2017

FEMA
Office of the Chief Administrative Officer
Information Management Division (FOIA Appeals)
500 C St SW, Seventh Floor, Mail Stop 3172
Washington, D.C. 20472-3172

Dear Madam or Sir:

This is an appeal under the Freedom of Information Act (FOIA) of your decision to withhold four records (records [1] - [4] below) of the Strategic National Risk Assessment (SNRA). You released three additional records ([6] – [8]). One record, the 2011 PPD-8 Implementation Plan ([5]), remains under review.

- The four withheld records were withheld pursuant to exemption 5, under the deliberative process privilege.
- You determined there were no security or information sensitivity issues that would otherwise prevent the requested records from public release.
- No other FOIA interest was cited.

The SNRA is the strongest, most rigorous, most objective tool for informing investment decisions across all hazards that FEMA possesses. Its quantitative method makes our planning assumptions explicit in a way that makes it possible for any expert, critic, or citizen to examine and question them, to an extent that no other kind of analysis that we practice can do.

That quantitative method also opens up the SNRA for many additional users and uses across the enterprise. It offers a uniform, auditable, repeatable method for assessing risk across all hazards that jurisdictional planners and emergency managers, infrastructure operators, business owners, schools, museums, places of worship, communities, families, and citizens can use to understand and communicate their risks in a common language not available to them today.

The SNRA is the only tool in the world that is capable of being used – right now – to inform cost-benefit tradeoff decisions across every Department in the U.S. Government.

We claim the SNRA as the objective basis of the National Preparedness System. But we have not submitted it to the critical and stakeholder scrutiny that U.S. Government policy requires; that we committed to; that is central to our doctrine; and that it needs to ensure that it is sound enough for us and our many partners to use.

Appeal

A deliberative product cannot be claimed as supporting evidence for final public policy, without losing its deliberative process protection.

In particular, disclosure is required where a decision-maker has referred to an intra-agency memorandum as a *basis* for his decision. Once adopted as a rationale for a decision, the memorandum becomes part of the public record.[1]

> The Strategic National Risk Assessment indicates that a wide range of threats and hazards continue to pose a significant risk to the Nation, affirming the need for an all-hazards, capability-based approach to preparedness planning.
>
> *- National Preparedness Goal, 2nd ed.*

When the cited evidence is presented as being scientific or technical in nature, as the SNRA is, the agency has a positive obligation to pro-actively push it out to public and critical scrutiny under the Government-wide standards of the Information Quality Act. These requirements increase in proportion to the scope and importance of the decisions that an analysis is used to justify.[2]

We do not describe the SNRA's findings as deliberative products of a policy making process, based on priorities which can changed in an election. We assert them to be facts of the world, which can't.

We claim that these facts are evidenced by math and science. We claim that they are not within our deliberative power to wish or decide away, but must be dealt with. And we claim that our chosen policy approach follows from the recognition of these facts.

This use of the SNRA as evidence puts the policy claims that depend on it off-limits to the political scrutiny that normally enforces accountability in a democratic system. Reasonable people can disagree with policy priorities. Only ignorant people disagree with facts.

But this is why our use of the SNRA in this way obligates us to ensure that the means for ensuring accountability that science in the Government relies upon in place of elections – peer, public, stakeholder, and Congressional review – are applied to this very large, very technical instrument that we are claiming as justification for so many non-technical things.

We have not done this.

Our failure to do this, given every reason why we should have done so long ago, and no real good reason why we have not, has prevented the socialization and many uses of the SNRA that the U.S. national risk assessment was intended to serve.

FEMA's 2015 revision of the SNRA focused on removing obstacles to its circulation, and making it more useful to more people. My team worked very hard to make this highly sophisticated but little-seen technical product into a broadly accessible planning tool that FEMA's state, local, tribal, territorial, and whole community stakeholders could actually *use* as the shared risk basis of the National Preparedness System that we claimed it to be.

It still hasn't gotten to them.

---

[1] *National Council of La Raza et al. v. U.S. Department of Justice*, 411 F.3d 350, 358 (2nd Cir. 2005) ([15]), citing *Montrose Chemical Co. v. Train*, 491 F.2d 63, 70 (D.C. Cir. 1974) ([14]).

[2] The Information Quality Act and its SNRA context are discussed below.

Except for a conclusion, text boxes, and a reference to the last Administration changed from present to past tense, the remaining discussion is reproduced from my October 2016 request without modification.

> The SNRA provides an objective basis for understanding the greatest threats based on existing data and historical information.
>
> *- 2016 Response Federal Interagency Interoperational Plan*

Status of requested records

Withheld under Exemption 5:

1) **SNRA 2015 Findings** [Report], May 2015 (26 pages).
2) **SNRA 2015 Technical Appendix**, May 2015 (452 pages), including both parts:
   a. Front matter with 2015 added material (238 pages), pp. i-234; and the
   b. SNRA 2011 Unclassified Documentation of Findings (214 pages), pp. 235-448.
3) **SNRA 2015 Working Papers**, May 2015 (153 pages).
4) **SNRA Terms of Reference**, June 2011 (2 pages).

Still under review:

5) **PPD-8 Implementation Plan**, May 2011 (13 pages).

Released:

5) SNRA 2015 Update Background and General Guidance, February 2015 (3 pages).

6) SNRA 2015 Qualitative Data Instructions, February 2015 (6 pages).

7) SNRA 2015 Risk Summary Sheet Instructions & Template, February 2015 (34 pages).

These records comprise the unclassified documentation needed to understand and substantially replicate the findings of the SNRA as disseminated to the public in the 2015 National Preparedness Goal, 2nd edition, 30 September 2015, the five revised National Planning Frameworks, 16 June 2016; and the four public revised Federal Interagency Operational Plans (FIOPs), 18 August 2016.

Exemptions 1, 3, 7

Your review has already cleared the requested records for any security or information sensitivity issues, so I will not repeat my discussion of them here.

Exemption 5

Please note that Exemption 5 does not apply to material that is factual, as opposed to opinions or recommendations;[3] or analyses, whether deliberative or not, which have been expressly adopted in support of making a final decision.[4]

With the possible exception of some segregable portions of the Working Papers, the requested records are neither deliberative nor pre-decisional.

> The SNRA relied on the best available quantitative estimates of frequency and consequence from existing Government assessments, peer-reviewed literature, and expert judgment.
>
> *- SNRA 2011 public summary*

1) The requested records are not deliberative, in claim or in fact.

   FEMA expressly claims the SNRA as the risk basis[5] of – and justification for[6] – the National Preparedness System (NPS). FEMA further makes it very clear that the SNRA's authority, as objective, apolitical supporting evidence for the deliberative policy decisions that determined the NPS, comes from the non-deliberative nature of the SNRA's analysis.[7]

---

[3] *Environmental Protection Agency* et al. *v. Mink* et al, 410 U.S. 73 (1973) ([12]) at 837; note 27, *National Labor Relations Board et al. v. Sears, Roebuck & Co*., 421 U.S. 132, 152-154 (1975) ([16]) at 161; *Heartwood v. U.S. Forest Service*, 431 F. Supp. 2d 28 (D. D.C. 2006) ([13]) at 37; *Chicago Tribune Co. v. U.S. Department of Health and Human Services*, 1997 U.S. Dist. LEXIS 2308 (N.D. Ill. Feb. 26, 1997) ([11]) at 52-53.

[4] *Sears v. NLRB* (1975) ([16]) 421 U.S. 132 at 152-154; *Coastal States Gas Corporation v. Department of Energy,* 617 F.2d 854, 866 (D.C. Cir. 1980) ([10]); *National Council of La Raza et al. v. U.S. Department of Justice*, 411 F.3d 350, 358-359 (2nd Cir. 2005) ([15]).

[4] "[D]isclosure is required 'where a decision-maker has referred to an intra-agency memorandum as a *basis* for his decision,' since 'once adopted as a rationale for a decision, the memorandum becomes part of the public record.'" *La Raza*, 411 F.3d at 358 ([15]), citing *Montrose Chemical Co. v. Train*, 491 F.2d 63, 70 (D.C. Cir. 1974) ([14]) (emphasis in citing case).

[5] DHS (2016b) ([55]) 4, DHS (2016c) ([56]) 5, DHS (2016d) ([57]) 6, DHS (2016e) ([58]) 7, 20, DHS (2016f) ([59]) 8, DHS (2016h) ([61]) 6, DHS (2016i) ([62]) 7.

[6] DHS (2015) ([53]) 4.

[7] FEMA presents the SNRA as based in a very different kind of authority – one that is technical and factual in nature, and governed by its own set of rules – than the deliberative, policy-making authority behind the doctrinal and planning documents that rely on the SNRA for their risk basis. This narrative is especially emphasized in the public description of the SNRA on FEMA's website (*The Strategic National Risk Assessment in Support of PPD-8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation:* at https://www.fema.gov/media-library/assets/documents/29223 [DHS (2011e) ([40])]). The five pages of text in this short document give very little actual content. However, they are steeped in the language of science, and repeated assertions of the SNRA's objective, quantitative nature.

The SNRA findings are derived with math:

> The results of the SNRA… include a comparison of risks for potential incidents in terms of the likelihood (**calculated** as a frequency)… (p. 4) (emphasis added)

The SNRA is based on facts, models, data, and objective methods from multiple fields of scholarly endeavor:

> The SNRA drew **data** and **information** from a variety of sources, including existing Government **models** and **assessments**, historical **records**, structured **analysis**, and judgments of **experts** from different **disciplines**… (p. 5) (emphasis added)

These assertions are true. The SNRA, and the requested records which document its unclassified data and analysis, is not deliberative because it is technical and factual in nature.[8,9] The purpose of the SNRA was to assess risks – not to make recommendations for how they should be managed.[10,11]

The SNRA simply asks

- With what frequency is it estimated that an event will occur?
- What are the impacts of the event(s) if it does occur?[12]

> FEMA is not seeking unsubstantiated opinions. All updated threats, hazards and findings which differ from the 2011 SNRA must be supported by quantitative data, qualitative data, or multiple subject matter expert statements supporting these opinions.
>
> *- SNRA 2015 Instructions to Contributors: General Guidance*

The SNRA's authority is not political or subjective, but based in hard numbers:

> The SNRA relied on the **best available quantitative estimates** of frequency and consequence from existing Government **assessments**, **peer-reviewed literature**, and **expert** judgment… (p. 6) (emphasis added)

And the SNRA is replicable, and backed by detailed documentation:

> All sources and estimates were **documented** to promote **credibility**, **defensibility**, and **transparency** within the assessment. (p. 6) (emphasis added)

[8] *EPA v. Mink*, 410 U.S. 73 at 837; see also note 27, *Sears*, 421 U.S. ([16]) at 161.

[9] *Heartwood*, 431 F. Supp. 2d ([13]) at 37.

[10] SNRA Terms of Reference (requested [withheld] record no. [5]); SNRA 2015 Update Background and General Guidance (released record no. [6]).

[11] For a number of reasons, accidental and intentional, the SNRA is a "pure" risk assessment uncontaminated by the risk management decisions it was first designed to inform. One reason is that FEMA senior leadership aggressively protected the SNRA from political influences. Others related to the SNRA's unusual decision context: since it needed to be able to support a multiplicity of diverse decision contexts, decisions, and decision-makers, the SNRA could not be customized to any one of them if it was to keep its utility to the rest. The core SNRA adopted a method that, by definition, produces results that are independent of the decision context for which they were originally calculated (DHS Risk Lexicon (2010) ([35]) 25, *Quantitative Risk Assessment Methodology*).

Since FOIA deliberative/non-deliberative determinations often turn on this point (whether or not an analysis is separable from its original decision context) and because the pervasiveness of references to the SNRA as a special authority in foundational National Preparedness System documents may otherwise cause confusion, it is important to recognize the strong degree of separation from any one decision context of the SNRA as an assessment in itself.

[12] DHS (2011e) ([40]) 5. Together with the initial risk identification step (*ibid.* 2, 4), these correspond to the three questions of classical risk analysis (Kaplan & Garrick (1980) ([29]) 13):

> 1) What can happen? (i.e., What can go wrong?)
>
> 2) How likely is it that that will happen?
>
> 3) If it does happen, what are the consequences?

The SNRA answers these questions – and stops there.

against a static background of the world as it exists today. It does not consider the effects of any policy or risk management alternatives upon that static background. It does not intrude into normative or policy judgements or suggestions of any kind:

> No effort was made to create a single "risk judgment" for any event type, because it was deemed infeasible to aggregate all impact types into a single metric. Instead, the assessment treated impact categories separately (e.g. economic impacts are reported separately from fatality impacts). This allowed stakeholders to apply their own expert judgments to the findings and decide how those findings should inform the Goal.[13]

Data providers should expect that the risk summary sheets documenting the source data and analysis supporting their top level estimates will be scrutinized by the public, experts in the U.S. risk technical community, and state, local, tribal, and territorial planners and emergency managers.

- SNRA 2015 Risk Summary Sheet Instructions & Template

As a risk assessment, two very important aspects of the SNRA are 1) its clear recognition that value and policy judgements belong to the end users of the assessment, not the analyst; and 2) its refusal to cross that bright line. More than any other property or content of the SNRA, it is this restraint from intruding into the decisions that it was meant to objectively inform that makes it uniquely suitable for the broad diversity of users[14] and uses[15] that it must serve as the risk assessment supporting the National Preparedness System.

[13] DHS (2011e) ([40]) 6.

[14] Note the SNRA's use of "stakeholders" in the plural. The unusual decision context of the SNRA – in particular, the participation of jurisdictional and whole community partners in the deliberative decisions that shaped the Goal (FEMA (2012) ([19]) 3, FEMA (2015c) ([23]) 1) – structured the SNRA in a number of ways different from a risk assessment intended for a specific, unitary decision-maker with a clearly defined decision to make. In the latter instance, where the assessment's primary function is customized decision support, a closer integration between risk assessment and risk management can be more appropriate than the separation that characterized the SNRA. DHS (2011b) ([37]) 22 (*Integrating Alternatives*).

[15] Including informing national capability targets (DHS (2011c) ([38]) 4); national capability investments (DHS (2011e) ([40]) 7); capability-based analysis (DHS (2016g) ([60]) 6); regional, state, and local risk assessments (PPD-8 Implementation Plan (record under review no. [5])) 2; SNRA Terms of Reference (withheld record no. [5]) IV); FEMA response planning (FEMA (2015a) ([21]) 7); FEMA resource allocation (DHS (2016i) ([62]) B-4); a national training and education system (DHS (2012b) ([42]) 52); national risk prioritization (White House (2015) ([66]) 1); and resource allocation for the Nation's global nuclear detection architecture (DHS (2014e) ([52]) 3).

2) The requested records are not pre-decisional, because they document an analysis that has been expressly adopted by the agency as an authority for final decisions,[16,17] on multiple occasions,[18] to the public.[19]

[16] *Sears* ([16]) at 152-154 ([16]).

[17] *Coastal States,* 617 F.2d at 866 ([10]).

[18] An agency cannot develop a body of 'secret law', used in its dealings with the public, but hidden behind a veil of privilege because it is not designated as 'formal', 'binding', or 'final'. "[T]hese opinions were routinely used by agency staff as guidance…and were retained and referred to as precedent. If this occurs, the agency has promulgated a body of secret law which it is actually applying in its dealings with the public but which it is attempting to protect behind a label. This we will not permit the agency to do. Tentative opinions are not relied on as precedent..." *Coastal States,* 617 F.2d ([10]) at 867, 869 (citations omitted) (emphasis added).

[19] *La Raza* (2005) ([15]) at 358-359.

FEMA claims the SNRA as the risk basis of the National Preparedness System,[20] and the justification for its all-hazards, capability-based doctrine.[21] If FEMA considers the SNRA to be draft or pre-decisional, it is nowhere described that way in its communications with Congress[22, 23,24,25,26] or the public.[27,28,29,30,31,32,33,34,35,36,37,38] Nor has it ever been.[39,40,41,42,43,44,45,46,47,48]

[20] DHS (2016b-j) ([55] – [59]).

[21] DHS (2015) ([53]). Each of the two iterations of the National Preparedness System has a corresponding iteration of the SNRA (DHS (2011c) ([38]) 3-4; FEMA (2015b) ([22]) 4, DHS (2015) ([53]) 4-5): each iteration (DHS (2011c) ([38]) 3; DHS (2015) ([53]) 4) has made this claim.

[22] FEMA (2012) ([19]).

[23] DHS (2012b) ([42]).

[24] FEMA (2014) ([20]).

[25] FEMA (2015a) ([21]).

[26] FEMA (2016) ([24]).

[27] DHS (2011e) ([40]) SNRA public summary.

[28] DHS (2013d) ([47]) Threat and Hazard Identification and Risk Assessment Guide: Comprehensive Preparedness Guide (CPG) 201, 2nd edition, 20.

[29] DHS (2015) ([53]) National Preparedness Goal, 2nd edition, 4-5.

[30] DHS (2016b) ([55]) National Prevention Framework, 2nd edition, 4-5, 23, 25.

[31] DHS (2016c) ([56]) National Protection Framework, 2nd edition, 5-6.

[32] DHS (2016d) ([57]) National Mitigation Framework, 2nd edition, 6-7.

[33] DHS (2016e) ([58]) National Response Framework, 3rd edition, 7-8, 20.

[34] DHS (2016f) ([59]) National Disaster Recovery Framework, 2nd edition, 8-9, 24.

[35] DHS (2016g) ([60]) Protection Federal Interagency Operational Plan (FIOP) 5-6.

[36] DHS (2016h) ([61]) Mitigation FIOP, 2nd edition, 5-6, A-5.

[37] DHS (2016i) ([62]) Response FIOP, 2nd edition, 7-8, B-3-4, B-9, B-1.1-1.4.

[38] DHS (2016j) ([63]) Recovery FIOP, 2nd edition, 5.

[39] DHS (2011c) ([38]) National Preparedness Goal, 1st edition, 3-4.

[40] DHS (2011d) ([39]) National Preparedness System Description, 2. This document comes the closest to describing the SNRA in a way that could be understood as non-final (by describing it in the present rather than the past tense).

[41] DHS (2012c) ([43]) CPG 201, 1st edition, 17.

[42] DHS (2013a) ([44]) National Mitigation Framework, 1st edition, 5-7.

[43] DHS (2013b) ([45]) National Prevention Framework, 1st edition, 4-5, 22, 25.

[44] DHS (2013c) ([46]) National Response Framework, 2nd edition, 7, 20.

[45] DHS (2014a) ([48]) National Protection Framework, 1st edition, 5-6.

[46] DHS (2014b) ([49]) Mitigation FIOP, 1st edition, 5-6, A-4.

[47] DHS (2014c) ([50]) Response FIOP, 1st edition, 6, B-3, B-4, B-8, B-1.1-3, X-62.

[48] DHS (2014d) ([51]) Recovery FIOP, 1st edition, 3.

- Once an agency expressly adopts an analysis as justification for policy decisions, its reasoning becomes the agency's to defend.[49]

> The 2015 SNRA will follow FEMA and U.S. Government information quality standards for highly influential scientific assessments of risk to health, safety, or the environment which are used to inform public policy.
>
> *- SNRA 2015 Risk Summary Sheet Instructions & Template*

Public and agency interest[50]

The requested documentation was written to ensure that FEMA could defend the SNRA, and everything that relies on it.[51]

The 2015 SNRA explicitly adopted the peer and stakeholder review requirements of OMB's information quality standards for U.S. Government risk assessments as its primary means of quality control.[52,53] These standards describe what needs to be included in the public documentation of publicly disseminated findings.

> [T]he agency needs to identify the sources of the disseminated information (to the extent possible, consistent with confidentiality protections) and, in a scientific, financial, or statistical context, the supporting data and models, so that the public can assess for itself whether there may be some reason to question the objectivity of the sources.[54]

The public technical documentation of publicly disseminated findings must explain the data, models, and methods that were used to derive them, in sufficient detail that they could be substantially reproduced.

> If an agency is responsible for disseminating influential scientific, financial, or statistical information, agency guidelines shall include a high degree of transparency about data and methods to facilitate the reproducibility of such information by qualified third parties…

---

[49] *Sears* ([16]) 421 U.S. at 152, 161.

[50] A government employee (I contributed to the 2011 SNRA and was technical lead for the 2015 iteration) may petition his own agency if 1) it is in the public interest, 2) it is consistent with law and policy, and 3) the public interest outweighs any negative impact to the agency's interest (*Borough of Duryea, Pennsylvania,* et al. *v. Guarnieri*, 564 U.S. 379 (2011) ([9])). This part addresses these criteria (this request is in the public interest, is directed to ensuring the completion of USG policy requirements on the SNRA, and is in FEMA's positive interest).

FOIA is the appropriate administrative mechanism for requests to provide (rather than correct) information under the Information Quality Act (IQA). OMB (2004a) ([32]) 51.

[51] DHS (2011e) ([40]) 6.

[52] SNRA 2015 Risk Summary Sheet Instructions & Template (released record [8]) 2-6.

[53] OMB (2002) ([31]), OMB (2004b) ([33]), OMB/OSTP (2007) ([34]). These standards implement OMB's interpretation of the Information Quality Act ([28]). A brief overview of the IQA standards in the context of the SNRA is provided on pp. 2-5 of the SNRA 2015 Risk Summary Sheet Instructions ([8]). A fuller overview is included with this letter for the reader's convenience (Attachment A).

[54] OMB (2002) ([31]) V.3.a, p. 8459. OMB defines "information" as

> any communication or representation of knowledge such as facts or data, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. This definition includes information that an agency disseminates from a web page, but does not include the provision of hyperlinks to information that others disseminate. This definition does not include opinions, where the agency's presentation makes it clear that what is being offered is someone's opinion rather than fact or the agency's views. (OMB (2002) ([31]) 8460 V.5)

> [A]gency guidelines shall generally require sufficient transparency about data and methods that an independent reanalysis could be undertaken by a qualified member of the public.[55]

They also set a positive standard of utility to the public:

> In assessing the usefulness of information that the agency disseminates to the public, the agency needs to consider the uses of the information not only from the perspective of the agency but also from the perspective of the public.
>
> As a result, when transparency of information is relevant for assessing the information's usefulness from the public's perspective, the agency must take care to ensure that transparency has been addressed in its review of the information.[56]

> The success and credibility of science are anchored in the willingness of scientists to expose their ideas and results to independent testing and replication by others.
>
> *- What is science? American Physical Society, 1999*

OMB's instructions do no more than make explicit the customary standards by which quantitative fields hold themselves accountable.[57,58] Their purpose is to ensure that these standards are enforced when the Government wishes to claim quantitative information as evidence for public policy.[59] They have three implications for the SNRA:

1) The SNRA documentation was written to make sure that the SNRA *could* be defended.

   However, for the SNRA to actually *be* defensible, it has to be seen. Scrutiny is the essential mechanism for quality control of technical work,[60] especially for very large, complex analyses like the SNRA. It is very much in FEMA's interest that the risk assessment that its plans are based on gets this examination.

   This examination needs to include not only experts, but also the public.[61] The SNRA's uncompromising rigor can be a powerful and clarifying discipline for understanding risk: but

> Scientists expect to have their data reviewed by other experts in the field in order to ensure the integrity of the results.
>
> *- Chicago Tribune v. HHS, 1997 Dist. LEXIS 2308*

---

[55] OMB (2002) ([31]) V.3.b.ii, V.3.b.ii.B, p. 8460.

[56] OMB (2002) ([31]]) V.2 p. 8459.

[57] The success and credibility of science are anchored in the willingness of scientists to

1) Expose their ideas and results to independent testing and replication by others. This requires the open exchange of data, procedures, and materials.
2) Abandon or modify previously accepted conclusions when confronted with more complete or reliable experimental or observational evidence.

Adherence to these principles provides a mechanism for self-correction that is the foundation of the credibility of science. (American Physical Society (1999) ([17]), "What is science?")

[58] *Chicago Tribune v. HHS*, 1997 U.S. Dist. LEXIS 2308 ([11]) at 52-53.

[59] We see reproducibility as an essential feature of competent and accountable government: show me what numbers, assumptions and equations you used and then show me how they add up to what you say they add up to! (Graham (2002) ([25]) 10)

[60] E.g. notes 57-59 above; OMB (2002) ([31]]) p. 8457 cols. 1-2 bridging paragraph.

[61] *Principles for Risk Communication,* OMB/OSTP (2007) ([34]) 10-13; DHS (2012c) ([43]) 17.

it can also lead to rigid thinking. Broader socialization would make it possible to reality-check the quantitative inputs of the SNRA against the common-sense judgment of emergency managers, community leaders, and real people outside the Beltway. Like any risk assessment, the SNRA needs to pull in a wide range of perspectives to avoid the traps of groupthink and conventional wisdom.[62]

> All levels of government and the whole community should assess and present risk in a similar manner to provide a common understanding of the threats and hazards confronting our Nation.
>
> *- National Preparedness Goal, 2nd edition*

2) For the SNRA to be of more than limited use to FEMA's mission, its stakeholders have to be able to use it too. But they can't use what they can't see.[63]

   The SNRA and THIRA methods complement each other: where each is challenged, is where the other excels. As the two primary risk assessment approaches of the National Preparedness System, they were intended to work together.[64] The SNRA's disappearance caused them to diverge over time.[65]

   Putting the SNRA in the hands of its jurisdictional and whole community stakeholders, as a THIRA resource, would make it possible for them to identify and assess their risks against a national standard based in sound science.[66,67] And allowing the different risk assessment processes used by the National Preparedness System to talk to one another will allow all levels of government to assess risk in a similar manner, to a greater extent than is possible at present.[68]

3) Making it possible for National Preparedness System stakeholders to access the risk assessment upon which it is based will help FEMA secure buy-in for the continued growth and development of the National Preparedness System in its present form. It can be challenging to build a sustainable constituency for an evidence-based doctrine, if the evidence behind that doctrine cannot be seen.[69]

> Understanding risks from threats or hazards requires the tools and skills to identify threats and hazards and assess risks and resilience… The analysis should leverage the best available, forward-looking, and science-based data.
>
> *-Mitigation Federal Interagency Operational Plan, 2nd edition*

---

[62] DHS (2011b) ([37]) 18.

[63] HSAC (2016) ([27]) 23, first bullet.

[64] DHS (2011d) ([39]) 2, DHS (2011e) ([40]) 7, DHS (2012c) ([43]) 17, DHS (2013d) ([47]) 20.

[65] HSAC (2016) ([27]) 21-23.

[66] DHS (2015) ([53]) 12.

[67] DHS has defended the SNRA's methodology as sound (DAS Policy/Strategic Plans, p. 35 GAO (2011) ([64]) [the quantitative core of the HSNRA was relabeled the SNRA for PPD-8, DHS (2012a) ([41]) p. 65]), and adopted it for its own risk assessments (Cohn (2013) ([18]) 8-20; FEMA in GAO (2016) ([65]), note 22).

[68] DHS (2015) ([53]) 4.

[69] HSAC (2016) ([27]) 21, *Consistency* bullets.

Relevance

> When will Congress see a complete picture of national risk…?
>
> *- Sen. Landrieu, question for the record, April 2013*

Would broader socialization of the SNRA have helped in the present disasters?

Maybe not. The SNRA's approach to risk analysis stresses the importance of uncertainty and broad thinking, against overconfidence and a focus on the here and now. These things are essential for long range preparedness and planning. But they can paralyze decisive action in a crisis.

But if the SNRA is cleared for public circulation, it can get to its stakeholders. It can get to Congress. It can get to peer review. It can get the millions of eyes and diverse perspectives outside the Beltway that are needed to see the flaws and opportunities in it that we can't.

At a minimum, the SNRA's evidence base and its careful, mathematical approach to problem solving should help jurisdictions, Federal agencies, businesses, communities, families, and citizens prepare for the next catastrophe. They *will* help Congress allocate resources across the Government with powerful quantitative tools it has never had before. And given how much the SNRA and its tools are connected to everything we do – not just in claim, but in reality – it is hard to see how getting more eyes on them will not help us in some way too.

Thank you,

Andrew Janca, Ph.D.
andrew.janca@outlook.com
PO Box 76303
Washington, DC 20013
(202) 375-0023

Attachments

- Attachment A: Information Quality Act overview
- Unlinked references not in DHS library:
  - Hagmann, Jonas, and Myriam Dunn Cavelty (2012, February). National risk registers: Security scientism and the propagation of permanent insecurity. *Security Dialogue* 43(1) 79-96.
  - Kaplan, Stanley, and B. John Garrick (1981). On the quantitative definition of risk. *Risk Analysis* 1(1) article 1 (pp. 11-27).

References

> Results of the Strategic National Risk Assessment (SNRA)… indicate that a wide range of threats and hazards continue to pose a significant risk to the Nation, affirming the need for an all-hazards, capability-based approach to preparedness planning.
>
> *- 2016 National Prevention, Protection, Mitigation, Disaster Recovery Frameworks*
>
> *- 2016 Protection Federal Interagency Operational Plan*

Requested records (repeated)

1. **SNRA 2015 Findings** [Report], May 2015 (26 pages).
2. **SNRA 2015 Technical Appendix**, May 2015 (452 pages), including both parts:
   a. Front matter with 2015 added material (238 pages), pp. i-234; and the
   b. SNRA 2011 Unclassified Documentation of Findings (214 pages), pp. 235-448.
3. **SNRA 2015 Working Papers**, May 2015 (153 pages).
4. **PPD-8 Implementation Plan**, May 2011 (13 pages).
5. **SNRA Terms of Reference**, June 2011 (2 pages).
6. **SNRA 2015 Update Background and General Guidance**, February 2015 (3 pages).
7. **SNRA 2015 Qualitative Data Instructions**, February 2015 (6 pages).
8. **SNRA 2015 Risk Summary Sheet Instructions & Template**, February 2015 (34 pages).

Case law

9. *Borough of Duryea, Pennsylvania,* et al. *v. Guarnieri*, 564 U.S. 379 (2011).
10. *Coastal States Gas Corporation v. Department of Energy,* 617 F.2d 854, 866 (D.C. Cir. 1980).
11. *Chicago Tribune Co. v. U.S. Department of Health and Human Services*, 1997 U.S. Dist. LEXIS 2308 (N.D. Ill. Feb. 26, 1997).
12. *Environmental Protection Agency* et al. *v. Mink* et al, 410 U.S. 73 (1973).
13. *Heartwood v. U.S. Forest Service*, 431 F. Supp. 2d 28 (D. D.C. 2006).
14. *Montrose Chemical Co. v. Train*, 491 F.2d 63 (D.C. Cir. 1974)
15. *National Council of La Raza* et al. *v. U.S. Department of Justice*, 411 F.3d 350 (2nd Cir. 2005).
16. *National Labor Relations Board et al. v. Sears, Roebuck & Co*., 421 U.S. 132 (1975).

Other references

17. American Physical Society (APS) (1999, November 14). What is science? APS Council policy statement 99.6: at https://www.aps.org/policy/statements/99_6.cfm.
18. Cohn, Alan D. (2013, September 9). Using Enterprise-Wide Risk Modeling, Analysis, and Assessment to Inform Homeland Security Policy and Strategy. Office of Policy, U.S. Department of Homeland Security. Presentation, Association for Federal Enterprise Risk Management (AFERM) 6th Annual Federal Enterprise Risk Management Summit: Maximizing Risk-Informed Decision Making in a Period of Change and Uncertainty. George Mason University, Virginia: at http://www.aferm.org/alancohn-riskmodeling.pdf.
19. Federal Emergency Management Agency (2012, June 6). Written testimony, Timothy Manning, Deputy Administrator Protection and National Preparedness, FEMA, hearing "The National Preparedness Report:

Assessing the state of preparedness." House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications: at https://homeland.house.gov/files/Testimony-Manning.pdf.

20. Federal Emergency Management Agency (2014, July 24). Written testimony, Joseph Nimmich, Associate Administrator Office of Response and Recovery, FEMA, hearing "The path to efficiency: Making FEMA more effective for streamlined disaster operations." Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Emergency Management, Intergovernmental Relations, and the District of Columbia: at http://www.hsgac.senate.gov/download/?id=AE0D0AC9-1E36-4DFE-BDF0-22906A38CC33.

> The NRF leverages the results of the Strategic National Risk Assessment (SNRA)… The results indicate that a wide range of threats and hazards continue to pose a significant risk to the Nation, affirming the need for an all-hazards, capability-based approach to preparedness planning.
>
> *- National Response Framework, 3rd ed.*

21. Federal Emergency Management Agency (2015, June 10) (2015a). Written testimony, Robert J. Fenton, Deputy Associate Administrator Office of Response and Recovery, FEMA, hearing "Defense support of civil authorities: A vital resource in the Nation's homeland security missions." House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications: at http://docs.house.gov/meetings/HM/HM12/20150610/103575/HHRG-114-HM12-Wstate-FentonR-20150610.pdf.

22. Federal Emergency Management Agency (2015, September 16) (2015b). National Preparedness Directorate update: National Advisory Council briefing. Presentation: at http://www.fema.gov/media-library-data/1444157533088-97dcba5e34fddfd543c6401012b097b1/NPDUpdate_KatieFox_9-16-15(508c2).pdf.

23. Federal Emergency Management Agency (2015, September 30) (2015c). National Preparedness Goal, Second Edition – What's New. Information sheet: at https://www.fema.gov/media-library-data/1443703117389-27c542ca395218d3154e5c1dfa8bfcb6/National_Preparedness_Goal_Whats_New_2015.pdf.

24. Federal Emergency Management Agency (2016, April 12). Written testimony, Timothy Manning, Deputy Administrator Protection and National Preparedness, FEMA, hearing "FEMA: Assessing progress, performance, and preparedness." Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Spending Oversight and Emergency Management: at http://www.hsgac.senate.gov/download/manning-statement.

25. Graham, John D. (2002, March 21). OMB's role in overseeing information quality. Remarks, Public Workshop on Information-Quality Guidelines, National Academy of Sciences. OMB Office of Information and Regulatory Affairs (OIRA): at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/info-quality_march21.pdf

26. Hagmann, Jonas, and Myriam Dunn Cavelty (2012, February). National risk registers: Security scientism and the propagation of permanent insecurity. *Security Dialogue* 43(1) 79-96.

27. Homeland Security Advisory Council (2016). Grant Review Task Force: final report, spring 2016. At https://www.dhs.gov/sites/default/files/publications/HSAC%20-%20Grant%20Review%20Task%20Force%20-%20Final%20Report%20-%20FINAL%20(accessible).pdf.

28. Information Quality Act. Section 515, Consolidated Appropriations Act for FY 2001 (Public Law 106-554); at http://www.fws.gov/informationquality/section515.html.

29. Kaplan, Stanley, and B. John Garrick (1981). On the quantitative definition of risk. *Risk Analysis* volume 1, issue 1, article 1 (pp. 11-27).

30. Landrieu, Mary (2013, April 23). Question for the record. Department of Homeland Security Appropriations for Fiscal Year 2014. Hearing, 23 April 2013, Senate Appropriations Committee, Homeland Security Subcommittee: at https://www.gpo.gov/fdsys/pkg/CHRG-113shrg59104614/html/CHRG-113shrg59104614.htm.

31. Office of Management and Budget (2002, February 22) (2002). Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies; Notice; Republication. *Federal Register* 67(36) 8452-8460; at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/fedreg/reproducible2.pdf.

32. Office of Management and Budget (2004, April 30) (2004a). Information Quality: a report to Congress, FY 2003. At https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/fy03_info_quality_rpt.pdf.

The SNRA affirmed the need for the Response FIOP's all-hazards, capability-based approach to preparedness planning.

- 2016 Response Federal Interagency Interoperational Plan

33. Office of Management and Budget (2004, December 16) (2004b). Final Information Quality Bulletin for Peer Review. At http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/peer_review041404.pdf.

34. Office of Management and Budget, Office of Science and Technology Policy (2007, September 19). Updated Principles for Risk Analysis: Memorandum to the Executive Branch; at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-24.pdf.

35. U.S. Department of Homeland Security (2010, September). DHS Risk Lexicon, 2010 edition. DHS Risk Steering Committee (RSC). At Risk Management Fundamentals: Homeland Security Risk Management Doctrine. Page 1. At https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

36. U.S. Department of Homeland Security (2011, March 18) (2011a). Information Quality Guidelines. At http://www.dhs.gov/sites/default/files/publications/dhs-iq-guidelines-fy2011.pdf.

37. U.S. Department of Homeland Security (2011, April) (2011b). Risk Management Fundamentals: Homeland Security Risk Management Doctrine. At https://www.dhs.gov/sites/default/files/publications/rma-risk-management-fundamentals.pdf.

38. U.S. Department of Homeland Security (2011, September) (2011c). National Preparedness Goal, 1st edition (2011). At http://www.fema.gov/media-library-data/20130726-1828-25045-9470/national_preparedness_goal_2011.pdf.

39. U.S. Department of Homeland Security (2011, November) (2011d). National Preparedness System Description. At http://www.fema.gov/media-library-data/20130726-1855-25045-8110/national_preparedness_system_final.pdf.

40. U.S. Department of Homeland Security (2011, December 9) (2011e). The Strategic National Risk Assessment in support of PPD 8: A comprehensive risk-based approach toward a secure and resilient Nation (public summary). At https://www.fema.gov/media-library/assets/documents/29223.

41. U.S. Department of Homeland Security (2012, February 3) (2012a). Alan D. Cohn, Office of Strategic Plans (DHS Office of Policy). Oral testimony, p. 65. Transcript, hearing "Is DHS effectively implementing a strategy to counter emerging threats?" House Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management: at https://www.hsdl.org/?view&did=731178.

42. U.S. Department of Homeland Security (2012b). Response to question for the record, hearing "Department of Homeland Security Appropriations for Fiscal Year 2013" 8 March 2012, p. 52. At http://www.appropriations.senate.gov/download/2014/09/26/hearing-record.

43. U.S. Department of Homeland Security (2012, April) (2012c). Threat and Hazard Identification and Risk Assessment Guide: Comprehensive Preparedness Guide (CPG) 201. 1st edition. At https://emilms.fema.gov/IS230c/assets/cpg_201_thira_guide.pdf.

44. U.S. Department of Homeland Security (2013, May 1) (2013a). National Mitigation Framework, 1st edition (2013). At http://purl.fdlp.gov/GPO/gpo47173.

45. U.S. Department of Homeland Security (2013, May 1) (2013b). National Prevention Framework, 1st edition (2013). At http://purl.fdlp.gov/GPO/gpo47172.

46. U.S. Department of Homeland Security (2013, May) (2013c). National Response Framework, 2nd edition (2013). At http://purl.fdlp.gov/GPO/gpo49580.

47. U.S. Department of Homeland Security (2013, August) (2013d). Threat and Hazard Identification and Risk Assessment Guide: Comprehensive Preparedness Guide (CPG) 201. 2nd edition. At http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf.

> The SNRA also affirms the need for the Recovery FIOP to incorporate an all-hazards, capability-based approach to preparedness planning.
>
> *- 2016 Recovery Federal Interagency Interoperational Plan*

48. U.S. Department of Homeland Security (2014, July 29) (2014a). National Protection Framework, 1st edition (2014). At http://purl.fdlp.gov/GPO/gpo51371.

49. U.S. Department of Homeland Security (2014, July 29) (2014b). Mitigation Federal Interagency Operational Plan (FIOP), 1st edition (2014). At https://web.archive.org/web/20141224065917/http://www.fema.gov/media-library/assets/documents/97356.

50. U.S. Department of Homeland Security (2014, July 29) (2014c). Response Federal Interagency Operational Plan (FIOP), 1st edition (2014). At https://web.archive.org/web/20150226034344/http://www.fema.gov/media-library-data/1406719953589-4ab5bfa40fe82879611d945dd60230c4/Response_FIOP_FINAL_20140729.pdf.

51. U.S. Department of Homeland Security (2014, July 29) (2014d). Recovery Federal Interagency Operational Plan (FIOP), 1st edition (2014). At http://web.archive.org/web/20160702111126/http://www.fema.gov/media-library-data/1406719669673-6081c9249705bc59153d724abcb2e7ca/Recovery_FIOP_FINAL_20140729.pdf.

52. U.S. Department of Homeland Security (2014, July 29) (2014e). Written testimony, Huban A. Gowadia, Director, Domestic Nuclear Detection Office. House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies: at http://docs.house.gov/meetings/HM/HM08/20140729/102498/HMTG-113-HM08-Wstate-GowadiaH-20140729.pdf.

53. U.S. Department of Homeland Security (2015, September 30). National Preparedness Goal, second edition (2015). At http://www.fema.gov/national-preparedness-goal.

54. U.S. Department of Homeland Security (2016, April 13 [last published date]) (2016a). DHS Information Quality Standards. At http://www.dhs.gov/information-quality-standards.

55. U.S. Department of Homeland Security (2016, June 16) (2016b). National Prevention Framework, 2nd edition (2016). At http://www.fema.gov/media-library-data/1466017209279-83b72d5959787995794c0874095500b1/National_Prevention_Framework2nd.pdf.

56. U.S. Department of Homeland Security (2016, June 16) (2016c). National Protection Framework, 2nd edition (2016). At http://www.fema.gov/media-library-data/1466017309052-85051ed62fe595d4ad026edf4d85541e/National_Protection_Framework2nd.pdf.

57. U.S. Department of Homeland Security (2016, June 16) (2016d). National Mitigation Framework, 2nd edition (2016). At http://www.fema.gov/media-library-data/1466014166147-11a14dee807e1ebc67cd9b74c6c64bb3/National_Mitigation_Framework2nd.pdf.

58. U.S. Department of Homeland Security (2016, June 16) (2016e). National Response Framework, 3rd edition (2016). At http://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf.

59. U.S. Department of Homeland Security (2016, June 16) (2016f). National Disaster Recovery Framework, 2nd edition (2016). At http://www.fema.gov/media-library-data/1466014998123-4bec8550930f774269e0c5968b120ba2/National_Disaster_Recovery_Framework2nd.pdf.

60. U.S. Department of Homeland Security (2016, August 18) (2016g). Protection Federal Interagency Operational Plan (FIOP), 1st edition (2016). At http://www.fema.gov/media-library-data/1471452730266-1811f70b81e59e75a48398d31f0ef2f6/Protection_FIOP_1st.pdf.

61. U.S. Department of Homeland Security (2016, August 18) (2016h). Mitigation Federal Interagency Operational Plan (FIOP), 2nd edition (2016). At http://www.fema.gov/media-library-data/1471450195109-d68f4bb054782a379b341999317bd123/Mitigation_FIOP_2nd.pdf.

The Strategic National Risk Assessment identified the threats and hazards that pose the greatest threat to the Nation and provided the basis for establishing the National Preparedness Goal and the core capability requirements for all mission areas.

- 2016 Mitigation Federal Interagency Interoperational Plan

62. U.S. Department of Homeland Security (2016, August 18) (2016i). Response Federal Interagency Operational Plan (FIOP), 2nd edition (2016). At http://www.fema.gov/media-library-data/1471452095112-507e23ad4d85449ff131c2b025743101/Response_FIOP_2nd.pdf.

63. U.S. Department of Homeland Security (2016, August 18) (2016j). Recovery Federal Interagency Operational Plan (FIOP), 2nd edition (2016). At http://www.fema.gov/media-library-data/1471451918443-dbbb91fec8ffd1c59fd79f02be5afddd/Recovery_FIOP_2nd.pdf.

64. U.S. Government Accountability Office (2011, September 15). Quadrennial Homeland Security Review: Enhanced stakeholder consultation and use of risk information could strengthen future reviews. GAO-11-873: at http://www.gao.gov/products/GAO-11-873.

65. U.S. Government Accountability Office (2016, April 15). Quadrennial Homeland Security Review: Improved risk analysis and stakeholder consultations could enhance future reviews. GAO-16-371: at http://www.gao.gov/products/GAO-16-371.

66. White House (2015, October). National Space Weather Strategy. National Science and Technology Council, Executive Office of the President: at https://www.whitehouse.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf.

-- This page blank --

Attachment 1. Information Quality Act overview

U.S. Government information policy requires scientific and technical works – in particular (but not limited to) risk assessments – that are not otherwise encumbered by classification, proprietary, or privacy issues to be made available to peer and public scrutiny before they are used to inform significant public policy or government decisions.

These standards ensure the quality and integrity of science used in the Executive Branch. When an agency chooses to rely on an analysis of some kind to justify a significant public policy decision, these standards limit the agency's ability to keep that analysis from public, technical, or legislative scrutiny.[1]

Context

Public Law 106-554, Section 515,[2] otherwise known as the Information Quality Act (or Data Quality Act) requires Federal agencies to issue guidelines ensuring and maximizing the quality, objectivity, utility, and integrity of information disseminated by the Federal Government. The Data Quality Act was enacted in December 2000 and builds on the Paperwork Reduction Act (PRA).[3]

These standards apply to "information that an agency disseminates, e.g., a risk assessment prepared by the agency to inform the agency's formulation of possible regulatory or other action."[4] In particular, these standards apply to influential scientific information. As defined by OMB,

> The term "influential scientific information" means scientific information the agency reasonably can determine will have or does have a clear or substantial impact on important public policies or private sector decisions. In the term "influential scientific information," the term "influential" should be interpreted consistently with OMB's government-wide information quality guidelines and the information quality guidelines of the agency.
>
> Information dissemination can have a significant economic impact even if it is not part of a rulemaking. For instance, the economic viability of a technology can be influenced by the government's characterization of its attributes. Alternatively, the Federal government's assessment of risk can directly or indirectly influence the response actions of state and local agencies or international bodies.
>
> One type of scientific information is a scientific assessment. For the purposes of this Bulletin, the term "scientific assessment" means an evaluation of a body of scientific or technical knowledge, which typically synthesizes multiple factual inputs, data, models, assumptions, and/or applies best professional judgment to bridge uncertainties in the available information. These assessments include, but are not limited to, state-of-science reports; technology assessments; weight-of-evidence analyses; meta-analyses; [or] health, safety, or ecological risk assessments… Such assessments often draw upon knowledge from multiple disciplines.[5]

Of these, risk assessments are the kind of scientific information that is most frequently used to inform U.S. Government policy-making. Risk analysis, based on objective science, is *the* key tool used to evaluate health, safety and environmental risks to inform policy-makers as to the extent to which different policy choices can reduce risks.[6] Risk analysis is the only kind of scientific information which has its own additional set of information quality guidelines;[7] the only kind for which OMB's standards can apply even to information that is not disseminated;[8] and the only kind with its own line item in the information quality compliance reports the Department sends to OMB every year.[9]

In a homeland security context, risk and risk analysis drive policy,

> The 2015 SNRA will follow FEMA and U.S. Government information quality standards for highly influential scientific assessments of risk to health, safety, or the environment which are used to inform public policy.
>
> *- SNRA 2015 Risk Summary Sheet Instructions & Template*

planning, doctrinal, resourcing, and operational decisions across the enterprise.[10] Because homeland security *is* national risk management,[11] risk assessment is the quantitative tool most frequently used to inform homeland security decisions.[12] As described by the National Academies,

> Risk analysis offers (1) a framework for applying scientific knowledge and the data to examine risk management decision making when the consequences of alternative decisions are uncertain and (2) a systematic method of revising decisions in the light of new information or events. The hazards to be analyzed (e.g. physical, chemical, nuclear, radiological, and biological agents) may result from natural events (e.g. hurricanes and earthquakes), technological events (e.g. chemical accidents), and human activity (e.g., the design and operation of engineered systems or an attack by a terrorist).[13]

From a public policy perspective, DHS' most ambitious analyses of this kind are its national risk assessments.[14] These must make comparative judgments between risks – chemical accidents vs. terrorist bombings, nuclear meltdowns vs. pandemics, geo-magnetic storms vs. a second 9/11 – touching the equities, responsibilities, and budgets of every Department in the U.S. Government.[15] This task requires the evaluation and synthesis of data and analysis from a very large number of scientific and technical disciplines, and from an even larger number of sources. These sources include peer-reviewed literature, existing Government models and analyses, and sometimes original research when pre-existing defensible data cannot be found.[16]

However, classified information is exempt from some of the more specific peer review process requirements of OMB's information quality guidance.[17,18] Although many countries publish their own national risk assessments in their entirety (figure 1) to enable public participation in their national preparedness planning,[19] to date, DHS' national risk assessments have been entirely classified works.[20]

---

[1] E.g. OMB (2004a) ([15]) pp. 9, 60-61, 112-117, 98, 54-55 (IQA uses by external scholars, the public, Members of Congress, and other USG agencies).

[2] IQA ([4]).

[3] DHS (2016a) ([33]).

[4] OMB (2002) ([14]) Supplementary Information, p. 8454 col. 1. Since risk assessments used in rulemakings already have a public quality challenge procedure in the Administrative Procedures Act, the primary utility of the IQA is for assessments used for non-regulatory actions. OMB (2005) ([17]) pp. 65-66.

[5] OMB (2004b) ([16]) Supplementary Information p. 2667 col. 3 (source first paragraph divided for readability).

[6] OMB (2010) ([17]) p. 57 (emphasis added).

[7] OMB/OSTP (2007) ([20]), OMB (2009) ([18]) pp. 48, 67-69.

[8] OMB (2002) ([14]) V.3.b.ii.C, p. 8460.

[9] E.g. DHS (2006) ([25]) sections III, IV.

[10] DHS (2011b) ([28]), DHS (2014) ([30]) (entire document).

[11] DHS (2014) ([30]) p. 32.

[12] Bennett (2008) ([1]), Klucking (2009) ([5]), NAS (2008) ([7]), NAS (2010) ([8]), DHS (2014) ([30]) pp. 15, 32.

[13] NAS (2008) ([7]) p. 11.

[14] NAS (2010) ([8]) p. 9, United States (2012) pp. 15-16, DHS (2016b) slide 4.

[15] DHS (2011c) ([29]), Cohn (2013) ([2]), GAO (2016) ([35]).

[16] DHS (2011c) ([29]) pp. 5-6.

[17] OMB (2004b) ([16]) IX.1, p. 2677. These require peer review of highly influential scientific information to be conducted according to a number of specified safeguards. Although these safeguards include public notice and transparency, the peer review requirement itself is distinct from and additional to the public transparency requirements specified elsewhere in OMB's information quality guidance (OMB (2004b) ([16]) p. 2665 col. 3).

Peer review most often takes place before an agency socializes information with the public. Reversing the order (public socialization before formal peer review) may be advisable when public participation is important to establish the credibility of the analytic process (OMB (2004b) ([16]) p. 2670 col. 3).

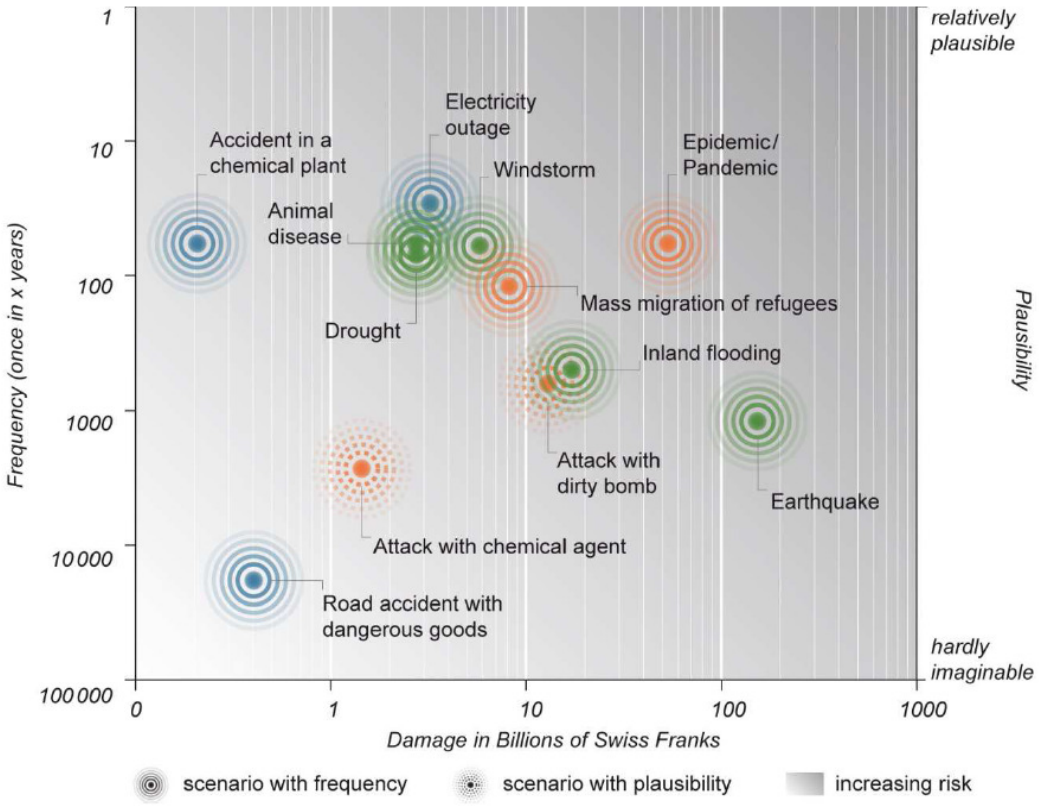
[18] OMB stresses that peer review is a testing process, not a determinative process:

> [W]hen a government agency sponsors peer review of its own draft documents, the peer review reports are an important factor in information dissemination decisions but rarely are the sole consideration. Agencies are not expected to cede their discretion with regard to dissemination or use of information to peer reviewers; accountable agency officials must make the final decisions. (OMB (2004b) ([16]) 2666 col. 1)

[19] Ireland (2012) ([5]), Netherlands (2009) ([9]), Norway (2013) [2012 assessment] ([10]), Sweden (2013) ([21]), Switzerland (2013) ([22]), Switzerland (2015a) ([23]), Switzerland (2015b) ([24]), UK (2013) ([36]). Norway did not estimate frequencies for terrorist attacks in its 2012 NRA (the only one with an English version), but provides them in Norway (2015) ([11]) (charts pp. 201-203, numbers to read charts in risk summary sheets). Hagmann and Cavelty (2012) ([3]) provide a critical review of national risk assessments.

[20] DHS (2011c) ([29]) p. 4. However, see Objectivity section below.

Figure 1. Example National Risk Assessment Frequency-Consequence Chart (Switzerland)[21]



[21] Switzerland (2015a) ([23]). Like those of most countries (but not the U.S.), Switzerland's national risk assessment aggregates fatality, injury, economic loss, environmental, and other consequences into a single consequence metric for its top level comparisons. Individual consequence measures are given in the threat/hazard risk summary sheets (Switzerland (2015b) ([24])) and methodology (Switzerland (2013) ([22])) (both in French). Willis et al (2012) ([38]) consider some of the issues with consequence aggregation in a study of the Netherlands' methodology. Hagmann and Cavelty (2012) ([3]) discuss some of the political issues with consequence aggregation and other aspects of national risk assessments in general (the SNRA, like other DHS risk assessments, does not aggregate consequences: this article was written before the publication of the SNRA public summary (DHS (2011c) ([29])).

Information Quality Act

The Information Quality Act directs OMB to issue policy and procedural guidance to Federal agencies for ensuring the quality, objectivity, utility, and integrity of information disseminated by the Federal Government. As interpreted by OMB, "quality" is the encompassing term, of which objectivity, integrity, and utility are constituents.

- Objectivity focuses on whether the disseminated information is being presented in an accurate, clear, complete, and unbiased manner; and as a matter of substance, is accurate, reliable, and unbiased.
- Integrity refers to security – the protection of information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.
- Utility refers to the usefulness of the information to the intended users.[22]

Objectivity

Objectivity involves two distinct elements: presentation and substance.[23]

Objectivity, in its presentation or communication element, includes whether disseminated information is being presented in an accurate, clear, complete, and unbiased manner.

- This includes identification of the sources of the disseminated information (to the extent possible, consistent with confidentiality protections) and, in a scientific, financial, or statistical context, the supporting data and models, so that the public can assess for itself whether there may be some reason to question the objectivity of the sources.
- Where appropriate, data should have full, accurate, transparent documentation, and error sources affecting data quality should be identified and disclosed to users.[24]

This transparency in presentation is not distinct from the requirement for objectivity in substance, but inherent to it.[25]

> If an agency is responsible for disseminating influential scientific, financial, or statistical information, agency guidelines shall include a high degree of transparency about data and methods to facilitate the reproducibility of such information by qualified third parties…
>
> [A]gency guidelines shall generally require sufficient transparency about data and methods that an independent reanalysis could be undertaken by a qualified member of the public. These transparency standards apply to agency analysis of data from a single study as well as to analyses that combine information from multiple studies.[26]

USG information quality guidance specific to risk analysis stresses that the legitimacy of a risk analysis used for public policy depends on the inclusion of public stakeholders as equal partners to technical experts:

1. Risk communication should involve the open, two-way exchange of information between professionals, including both policy makers and "experts" in relevant disciplines, and the public.
2. Risk management goals should be stated clearly, and risk assessments and risk management decisions should be communicated accurately and objectively in a meaningful manner. To maximize public understanding and participation in risk-related decisions, agencies should:
   a. Explain the basis for significant assumptions, data, models, and inferences used or relied on in the assessment or decision;
   b. Describe the sources, extent, and magnitude of significant uncertainties associated with the assessment or decision;
   c. Make appropriate risk comparisons, taking into account, for example, public attitudes with respect to voluntary versus involuntary risk; and
   d. Provide timely, public access to relevant supporting documents and a reasonable opportunity for public comment.[27]

[22] OMB (2002) ([14]) Supplementary Information p. 8453 cols. 2-3.

[23] OMB (2002) ([14]) V.3 p. 8459.

[24] OMB (2002) ([14]) V.3.a, p. 8459.

[25] See also DHS (2011b) ([28]), pp. 11-12, Transparency.

[26] OMB (2002) ([14]) V.3.b.ii, V.3.b.ii.B, p. 8460.

[27] OMB/OSTP (2007) ([20]) pp. 10-13; OMB (1995) ([13]) pp. 3-4. Quotation marks around "experts" in original (both versions).

> The 2015 project will rely on the peer and public review requirements of these standards as the primary means to ensure quality control for all material used to supplement, update, or revise the quantitative evidence base established by the 2011 SNRA.
>
> *- SNRA 2015 Risk Summary Sheet Instructions & Template*

Where full disclosure of the material is not possible because of security considerations, it is the obligation of the agency citing it in support of its policies, rules, or doctrine to ensure the objectivity of the information by rigorous peer review, conducted in an open and rigorous manner.[28]

> Making the data and methods publicly available will assist in determining whether analytic results are reproducible. However, the objectivity standard does not override other compelling interests such as privacy, trade secrets, intellectual property, and other confidentiality protections.
>
> In situations where public access to data and methods will not occur due to other compelling interests, agencies shall apply especially rigorous robustness checks to analytic results and document what checks were undertaken.[29]
>
> If data and analytic results have been subjected to formal, independent, external peer review, the information may generally be presumed to be of acceptable objectivity… If agency-sponsored peer review is employed to help satisfy the objectivity standard, the review process employed shall meet the general criteria for competent and credible peer review recommended by OMB-OIRA… [including that] "(d) peer reviews be conducted in an open and rigorous manner."[30]

However, even for sensitive scientific information for which peer review is substituted for full public disclosure,

> Agency guidelines shall, however, in all cases, require a disclosure of the specific data sources that have been used and the specific quantitative methods and assumptions that have been employed.[31]

Integrity

Integrity refers to the security of information – protection of the information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.[32]

The inherent relationship between quality and public scrutiny that the objectivity pillar stresses is shared with the integrity pillar. The last Administration's principal addition to the information quality standards, the 2009 scientific integrity memorandum, emphasizes this link:

> The public must be able to trust the science and scientific process informing public policy decisions. Political officials should not suppress or alter scientific or technological findings or conclusions. If scientific and technological information is developed and used by the Federal Government, it should ordinarily be made available to the public…
>
> Except for information that is properly restricted under disclosure under procedures established in accordance with statute, regulation, Executive Order, or Presidential Memorandum, each agency should make available to the public the scientific or technological findings considered or relied on in policy decisions.[33]

Utility

Utility refers to the usefulness of the information to its intended users, including the public.[34]

> In assessing the usefulness of information that the agency disseminates to the public, the agency needs to consider the uses of the information not only from the perspective of the agency but also from the perspective of the public.
>
> As a result, when transparency of information is relevant for assessing the information's usefulness from the public's perspective, the agency must take care to ensure that transparency has been addressed in its review of the information.[35,36]

[28] OMB (2002) ([14]) V.3.b.i, pp. 8459-8460.

[29] OMB (2002) ([14]) V.3.b.ii.B.i-ii, p. 8460.

[30] OMB (2002) ([14]) V.3.b.i, pp. 8459-8460 (presented out of order from preceding excerpt).

[31] OMB (2002) ([14]) V.3.b.ii.B.ii, p. 8460.

[32] OMB (2002) ([14]) V.4.

[33] Obama (2009) ([12]).

[34] DHS defines quantitative risk assessment methodology in terms of whether it is possible for other people to use its numbers for other purposes. DHS (2010) ([26]) p. 25.

[35] OMB (2002) ([14]) V.2 p. 8459.

References

1. Bennett, Steve (2008, June). WMD terrorism risk assessment in DHS Science & Technology. Science & Technology Directorate, U.S. Department of Homeland Security. Presentation, S&T Stakeholders Conference, June 2-5 2008: at http://www.dtic.mil/ndia/2008homest/benn.pdf.

2. Cohn, Alan D. (2013, September 9). Using Enterprise-Wide Risk Modeling, Analysis, and Assessment to Inform Homeland Security Policy and Strategy. Office of Policy, U.S. Department of Homeland Security. Presentation, Association for Federal Enterprise Risk Management (AFERM) 6th Annual Federal Enterprise Risk Management Summit: at http://www.aferm.org/alancohn-riskmodeling.pdf.

3. Hagmann, Jonas, and Myriam Dunn Cavelty (2012, February). National risk registers: Security scientism and the propagation of permanent insecurity. *Security Dialogue* 43(1) 79-96.

4. Information Quality Act. Section 515, Consolidated Appropriations Act for FY 2001 (Public Law 106-554); at http://www.fws.gov/informationquality/section515.html.

5. Ireland (2012, December). A National Risk Assessment for Ireland. Office of Emergency Planning, Department of Defence: at http://www.emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf.

6. Klucking, Sara (2009, October 6). DHS S&T Bioterrorism Risk Assessment (BTRA). Science & Technology Directorate, U.S. Department of Homeland Security. Presentation, International Symposium on Bioterrorism Risk, October 6-8 2009: at http://www.biosecurity.sandia.gov/ibtr/subpages/pastConf/20082009/albuquerque/6dhs3.pdf.

7. National Academies (2008). Department of Homeland Security Bioterrorism Risk Assessment. National Research Council, National Academies Press: at http://www.nap.edu/catalog/12206.html.

8. National Academies (2010). Review of the Department of Homeland Security's approach to risk analysis. National Research Council, National Academies Press: at http://www.nap.edu/catalog/12972.html.

9. Netherlands (2009, October). Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands (English). National Risk Strategy Annex 2, Ministry of the Kingdom and the Interior: at http://preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf.

10. Norway (2013, November 25). 2013 National Risk Analysis (English). Norwegian Directorate for Civil Protection: at http://old.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013_english.pdf.

11. Norway (2015). 2014 National Risk Analysis (Norwegian). Norwegian Directorate for Civil Protection: at https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2014.pdf.

12. Obama, Barack H. (2009, March 9). Scientific Integrity: Memorandum for the Executive Branch. At https://www.whitehouse.gov/the-press-office/memorandum-heads-executive-departments-and-agencies-3-9-09.

13. Office of Management and Budget (1995, January 12). At https://www.whitehouse.gov/sites/default/files/omb/assets/regulatory_matters_pdf/jan1995_risk_analysis_principles.pdf.

14. Office of Management and Budget (2002, February 22). Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies; Notice; Republication. *Federal Register* 67(36) 8452-8460; at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/fedreg/reproducible2.pdf.

15. Office of Management and Budget (2004, April 30) (2004a). Information quality: FY 2003 report to Congress. At https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/fy03_info_quality_rpt.pdf.

16. Office of Management and Budget (2004, December 16) (2004b). Final Information Quality Bulletin for Peer Review. At http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/peer_review041404.pdf.

17. Office of Management and Budget (2005, December). Implementation of the Information Quality Act. Chapter IV, Validating regulatory analysis: 2005 report to Congress on the costs and benefits of Federal regulations and unfunded mandates on state, local, and tribal entities. At https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/2005_cb/final_2005_cb_report.pdf.

18. Office of Management and Budget (2009, January 15). Update on the implementation of OMB's information quality initiatives. Chapter III, Report to Congress on the benefits and costs of Federal regulations and agency compliance with the Unfunded Mandates Reform Act, 208. At https://www.whitehouse.gov/sites/default/files/omb/assets/information_and_regulatory_affairs/2008_cb_final.pdf.

19. Office of Management and Budget (2010, January 27). Update on the implementation of OMB's information quality initiatives. Chapter IV, Report to Congress on the benefits and costs of Federal regulations and unfunded mandates on state, local, and tribal entities, 2009. At https://www.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/2009_final_BC_Report_01272010.pdf.

20. Office of Management and Budget, Office of Science and Technology Policy (2007, September 19). Updated Principles for Risk Analysis: Memorandum to the Executive Branch; at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-24.pdf.

21. Sweden (2013, June 12). Swedish National Risk Assessment 2012. Swedish Civil Contingencies Agency: at https://www.msb.se/RibData/Filer/pdf/26621.pdf.

22. Switzerland (2013, February 15). Rapport sur les risques 2012 (Risk Report 2012) (in French: English version is currently [5 October 2016] offline). Federal Office for Civil Protection (FOCP), Swiss Confederation: at http://www.babs.admin.ch/content/babs-internet/fr/publikationen-und-service/downloads/gefrisiken/_jcr_content/contentPar/accordion/accordionItems/diverse_unterlagen/accordionPar/downloadlist/downloadItems/122_1461071612919.download/knsrisikobericht2012fr.pdf.

23. Switzerland (2015, February) (2015a). The National Risk Assessment of Disasters and Emergencies in Switzerland: two-pager in English. Swiss Federal Office of Civil Protection (FOCP): at https://www.shareweb.ch/site/Disaster-Resilience/resilience-and-related-topics/Documents/FOCP_National-Risk-Assessment.pdf.

24. Switzerland (2015, June 30) (2015b). Swiss National Risk Assessment risk summary sheets (in French. *Attentats de types A, B, C* = rad/nuke, biological, chemical). Federal Office for Civil Protection (FOCP): at http://www.babs.admin.ch/fr/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html.

25. U.S. Department of Homeland Security (2006). 2006 Year-End Information Quality Report. At https://www.dhs.gov/xlibrary/assets/cio_infoqualityrpttemplatefy06.pdf.

26. U.S. Department of Homeland Security (2010, September). DHS Risk Lexicon. DHS Risk Steering Committee: at http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

27. U.S. Department of Homeland Security (2011, March 18) (2011a). Information Quality Guidelines. At http://www.dhs.gov/xlibrary/assets/dhs-iq-guidelines-fy2011.pdf.

28. U.S. Department of Homeland Security (2011, April) (2011b). Risk Management Fundamentals: Homeland Security Risk Management Doctrine. At https://www.dhs.gov/sites/default/files/publications/rma-risk-management-fundamentals.pdf.

29. U.S. Department of Homeland Security (2011, December 9) (2011c). The Strategic National Risk Assessment in support of PPD 8: A comprehensive risk-based approach toward a secure and resilient Nation (public summary). At http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf.

30. U.S. Department of Homeland Security (2014, June). Quadrennial Homeland Security Review 2014. DHS Office of Policy, Strategic Plans. At https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

31. U.S. Department of Homeland Security (2015, February 6/11) (2015a). Strategic National Risk Assessment (SNRA) 2015 Risk Summary Sheet Instructions and Template. Federal Emergency Management Agency, National Integration Center. FOIA release 3 August 2017 (record [8]).

32. U.S. Department of Homeland Security (2015, September 30) (2015b). National Preparedness Goal, second edition (2015). At http://www.fema.gov/national-preparedness-goal.

33. U.S. Department of Homeland Security (2016, April 13 [last published date]) (2016a). DHS Information Quality Standards. At http://www.dhs.gov/information-quality-standards.

34. U.S. Department of Homeland Security (2016, June 22) (2016b). Homeland Security National Risk Characterization. Presentation, Homeland Security Science and Technology Advisory Committee (HSSTAC) meeting 21-22 June 2016: at https://share.dhs.gov/p7csfuhdwur (downloadable deck).

35. U.S. Government Accountability Office (2016, April). Quadrennial Homeland Security Review: Improved risk analysis and stakeholder consultations could enhance future reviews. Report to Congressional requesters GAO-16-371; at http://www.gao.gov/products/GAO-16-371.

36. United Kingdom (2013, July 11). National Risk Register of Civil Emergencies. UK Cabinet Office. At https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211867/NationalRiskRegister2013_amended.pdf.

37. United States (2012, October 2). United States of America national progress report on the implementation of the Hyogo Framework for Action (2011-2013) – Interim. National Science and Technology Council (NSTC) Subcommittee on Disaster Reduction (SDR) [USG interagency committee]: at http://www.preventionweb.net/files/28816_usa_NationalHFAprogress_2011-13.pdf.

38. Willis et al (2012). The validity of the preference profiles used for evaluating impacts in the Dutch National Risk Assessment. RAND Corporation: at http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1278.pdf.

[36] DHS and FEMA risk doctrines take this principle one step further by making stakeholder use of the same risk tools as Federal risk managers a precondition for mission success. DHS (2011b) ([28]) Unity of Effort p. 11, DHS (2015b) ([**Error! Reference source not found.**]) "All levels…" p. 4.