

The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation

Overview

The Strategic National Risk Assessment (SNRA) was executed in support of Presidential Policy Directive 8 (PPD-8), which calls for creation of a National Preparedness Goal, a National Preparedness System, and a National Preparedness Report. Specifically, national preparedness is to be based on core capabilities that support “strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk¹ to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters.”

As part of the effort to develop the National Preparedness Goal and identify core capabilities, the Secretary of Homeland Security led an effort to conduct a strategic national risk assessment to help identify the types of incidents that pose the greatest threat to the Nation’s homeland security. Representatives from the offices of the Director of National Intelligence and the Attorney General, as well as other members of the Federal interagency, supported this effort. The assessment was used:

- To identify high risk factors that supported development of the core capabilities and capability targets in the National Preparedness Goal;
- To support the development of collaborative thinking about strategic needs across prevention, protection, mitigation, response, and recovery requirements, and;
- To promote the ability for all levels of Government to share common understanding and awareness of National threats and hazards and resulting risks so that they are ready to act and can do so independently but collaboratively.

The subsequent pages provide an overview of the unclassified findings and the analytic approach used to conduct the SNRA. It should be emphasized, however, that although the initial version of the SNRA is a significant step toward the establishment of a new homeland security risk baseline, it contains data limitations and assumptions that will require additional study, review, and revision as the National Preparedness System is developed. These limitations are discussed below, and future iterations of the assessment are expected to reflect an enhanced methodology and improved data sets.

Strategic National Risk Assessment Scope

To inform homeland security preparedness and resilience activities, the SNRA evaluated the risk from known threats and hazards that have the potential to significantly impact the Nation’s homeland security. These threats and hazards were grouped into a series of national-level events with the potential to test the Nation’s preparedness.

¹ The DHS Lexicon defines risk as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. Accessed at: <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>

SNRA participants – including Federal agencies, DHS Components, and the intelligence community, among others – developed a list of national-level events (see Table 1) for assessment in the initial SNRA. The events are grouped into three categories: 1) natural hazards; 2) technological/accidental hazards; and 3) adversarial, human-caused threats/hazards. For the purposes of the assessment, DHS identified thresholds of consequence necessary to create a national-level event. These thresholds were informed by subject matter expertise and available data. For some events, economic consequences were used as thresholds, while for others, fatalities or injuries/illnesses were deemed more appropriate as the threshold to determine a national-level incident. In no case, however, were economic and casualty thresholds treated as equivalent to one another (i.e., dollar values were not assigned to fatalities). Event descriptions in Table 1 that do not explicitly identify a threshold signify that no minimum consequence threshold was employed. This allows the assessment to include events for which the psychological impact of an event could cause it to become a national-level event even though it may result in a low number of casualties or a small economic loss. Only events that have a distinct beginning and end and those with an explicit nexus to homeland security missions were included. This approach excluded:

- Chronic societal concerns, such as immigration and border violations, and those that are generally not related to homeland security national preparedness, such as cancer or car accidents, and;
- Political, economic, environmental, and societal trends that may contribute to a changing risk environment but are not explicitly homeland security national-level events (e.g., demographic shifts, economic trends). These trends will be important to include in future iterations of a national risk assessment, however.

Table 1: SNRA National-Level Events

Threat/ Hazard Group	Threat/Hazard Type	National-level Event Description
Natural	Animal Disease Outbreak	An unintentional introduction of the foot-and-mouth disease virus into the domestic livestock population in a U.S. state
	Earthquake	An earthquake occurs within the U.S. resulting in direct economic losses greater than \$100 Million
	Flood	A flood occurs within the U.S. resulting in direct economic losses greater than \$100 Million
	Human Pandemic Outbreak	A severe outbreak of pandemic influenza with a 25% gross clinical attack rate spreads across the U.S. populace
	Hurricane	A tropical storm or hurricane impacts the U.S. resulting in direct economic losses of greater than \$100 Million
	Space Weather	The sun emits bursts of electromagnetic radiation and energetic particles causing utility outages and damage to infrastructure
	Tsunami	A tsunami with a wave of approximately 50 feet impacts the Pacific Coast of the U.S.
	Volcanic Eruption	A volcano in the Pacific Northwest erupts impacting the surrounding areas with lava flows and ash and areas east with smoke and ash
	Wildfire	A wildfire occurs within the U.S. resulting in direct economic losses greater than \$100 Million

Threat/ Hazard Group	Threat/Hazard Type	National-level Event Description
Technological/ Accidental	Biological Food Contamination	Accidental conditions where introduction of a biological agent (e.g., <i>Salmonella</i> , <i>E. coli</i> , botulinum toxin) into the food supply results in 100 hospitalizations or greater and a multi-state response
	Chemical Substance Spill or Release	Accidental conditions where a release of a large volume of a chemical acutely toxic to human beings (a toxic inhalation hazard, or TIH) from a chemical plant, storage facility, or transportation mode results in either one or more offsite fatalities, or one or more fatalities (either on- or offsite) with offsite evacuations/shelter-in-place
	Dam Failure	Accidental conditions where dam failure and inundation results in one fatality or greater
	Radiological Substance Release	Accidental conditions where reactor core damage causes release of radiation
Adversarial/ Human-Caused	Aircraft as a Weapon	A hostile non-state actor(s) crashes a commercial or general aviation aircraft into a physical target within the U.S.
	Armed Assault	A hostile non-state actor(s) uses assault tactics to conduct strikes on vulnerable target(s) within the U.S. resulting in at least one fatality or injury
	Biological Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponizes, and releases a biological agent against an outdoor, indoor, or water target, directed at a concentration of people within the U.S.
	Chemical/Biological Food Contamination Terrorism Attack	A hostile non-state actor(s) acquires, weaponizes, and disperses a biological or chemical agent into food supplies within the U.S. supply chain
	Chemical Terrorism Attack (non-food)	A hostile non-state actor(s) acquires, weaponizes, and releases a chemical agent against an outdoor, indoor, or water target, directed at a concentration of people using an aerosol, ingestion, or dermal route of exposure
	Cyber Attack against Data	A cyber attack which seriously compromises the integrity or availability of data (the information contained in a computer system) or data processes resulting in economic losses of a Billion dollars or greater
	Cyber Attack against Physical Infrastructure	An incident in which a cyber attack is used as a vector to achieve effects which are “beyond the computer” (i.e., kinetic or other effects) resulting in one fatality or greater or economic losses of \$100 Million or greater
	Explosives Terrorism Attack	A hostile non-state actor(s) deploys a man-portable improvised explosive device (IED), Vehicle-borne IED, or Vessel IED in the U.S. against a concentration of people, and/or structures such as critical commercial or government facilities, transportation targets, or critical infrastructure sites, etc., resulting in at least one fatality or injury

Threat/ Hazard Group	Threat/Hazard Type	National-level Event Description
	Nuclear Terrorism Attack	A hostile non-state actor(s) acquires an improvised nuclear weapon through manufacture from fissile material, purchase, or theft and detonates it within a major U.S. population center
	Radiological Terrorism Attack	A hostile non-state actor(s) acquires radiological materials and disperses them through explosive or other means (e.g., a radiological dispersal device or RDD) or creates a radiation exposure device (RED)

The SNRA participants identified the events listed in Table 1 as those with the potential to pose the greatest risk to the security of the Nation and formed the analytic basis of the SNRA. In some cases, tornados may also become national-level events that pose significant risk. Table 1 is not a complete list of risks that exist and will be reconsidered in future iterations of the assessment. Additional threats and hazards, such as droughts, heat waves, winter storms, rain storms, and different types of technological/accidental or human-caused hazards, can also pose a risk to jurisdictions across the country and should be considered, as appropriate, in preparedness planning. Non-influenza diseases with pandemic potential and other animal diseases should also be considered. In addition, assessment participants identified a number of events for possible inclusion in future iterations of the SNRA, including electric grid failure, plant disease outbreak, and transportation system failure.

Overarching Themes to an All-Hazards Approach

The results of the SNRA are largely classified and include a comparison of risks for potential incidents in terms of the likelihood (calculated as a frequency—i.e. number of events per year) and consequences of threats and hazards, as well as an analysis of the uncertainty associated with those incidents.² The assessment finds that a wide range of threats and hazards pose a significant risk to the Nation, affirming the need for an all-threats/hazards, capability-based approach to preparedness planning. Overarching themes include:

- Natural hazards, including hurricanes, earthquakes, tornadoes, wildfires, and floods, present a significant and varied risk across the country.
- A virulent strain of pandemic influenza could kill hundreds of thousands of Americans, affect millions more, and result in economic loss. Additional human and animal infectious diseases, including those previously undiscovered, may present significant risks.
- Technological and accidental hazards, such as dam failures or chemical substance spills or releases, have the potential to cause extensive fatalities and have severe economic impacts, and the likelihood of occurrence may increase due to aging infrastructure.

² The full results of the SNRA are classified.

- Terrorist organizations or affiliates may seek to acquire, build, and use weapons of mass destruction. Conventional terrorist attacks, including those by “lone actors” employing explosives and armed attacks, present a continued risk to the Nation.
- Cyber attacks can have their own catastrophic consequences and can also initiate other hazards, such as power grid failures or financial system failures, which amplify the potential impact of cyber incidents.

These findings supported the development of the core capabilities, as well as the establishment of capability targets for the Goal. In addition to the above findings articulated in the National Preparedness Goal, the SNRA found that:

- Many events have the potential to occur more than once every 10 years, meaning that the Nation’s preparedness will likely be tested in this decade.
- Although historic events provide a useful perspective on homeland security risks, the changing nature of society and the risk landscape means that the Nation must also be prepared for new hazards and threats or for events that result in greater consequences than have occurred in the past.
- Within an all-hazards preparedness context, particular events that present risk to the Nation—such as nuclear attacks or chemical releases—require additional specialized response activities.
- Some events, such as explosives attacks or earthquakes, generally cause more localized consequences, while other events, such as human pandemics, may cause consequences that are dispersed throughout the Nation, thus creating different types of impacts for preparedness planners to consider.

Analytic Approach

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. The information was used to assess the risk of identified incidents as a function of frequency³ and consequence—specifically, *With what frequency is it estimated that an event will occur, and what are the consequences of the incident(s) if it does occur?*

The SNRA examined the consequences associated with six categories of harm: loss of life, injuries and illnesses, direct economic costs, social displacement, psychological distress, and environmental impact. This multi-faceted view of potential consequences draws attention to the broad and often interdependent effects of incidents that require whole of community preparation and cooperation across the homeland security enterprise. For instance, community resilience relates to both mitigating human and economic consequences and addressing the psychological and social distress caused by the incident within the community. Similarly, other types of resilience involve withstanding environmental and infrastructure degradations to ensure that essential services continue to be delivered.

³ Frequency was used in the SNRA to capture likelihood because some events have the potential to occur more than once a year.

The SNRA relied on the best available quantitative estimates of frequency and consequence from existing Government assessments, peer-reviewed literature, and expert judgment. Where sufficient quantitative information was not available—such as data related to the frequency of high-consequence space weather—events were assessed qualitatively. The estimates of the frequency and consequences for each of the events considered were compared where appropriate. No effort was made to create a single “risk judgment” for any event type because it was deemed infeasible to aggregate all consequence types into a single metric. Instead, the assessment treated consequence categories separately (i.e., economic consequences are reported separately from fatality consequences). This allowed stakeholders to apply their own expert judgments to the findings and decide how those findings should inform core capability targets in the Goal.

All sources and estimates were documented to promote credibility, defensibility, and transparency within the assessment. Uncertainty in frequency and consequences was explicitly included in the analysis by representing low and high bounds in addition to best estimates. Examples of sources of uncertainty include incomplete knowledge of adversary capabilities and intent, variability in possible event severity and location, and lack of historical precedence.

Because the assessment was performed at a strategic national level, it provided the ability to draw rough comparisons of the assessed events—within an order of magnitude—to view the broad differences in risk across events. Given the uncertainty inherent in assessing risks at a national level and the lack of information about some of the events included—many of which are likely to occur very infrequently—the assessment was designed to avoid false precision. Instead, the assessment identifies only those differences in risk that are still significant despite the associated uncertainties.

Limitations

The analysis of available information—even if that analysis is imprecise and contains a wide degree of uncertainty—supports better decision making, as long as key limitations and assumptions are noted. Participants designed the SNRA to capture the best information the Nation has about homeland security risks to support the development of the National Preparedness Goal while recognizing the limitations of conducting such analysis in a shortened time frame.

- This is a *strategic national* risk assessment. As such, it does not present a full view of the risk facing local communities. To complement preparedness planning, it is necessary to consider national and regional risks, many of which differ from region to region.
- Given PPD-8’s emphasis on contingency events with defined beginning and endpoints (e.g. hurricanes, terrorist attacks), the current SNRA does not explicitly assess persistent, steady-state risks like border violations, illegal immigration, drug trafficking, and intellectual property violations, which are important considerations for DHS and the homeland security enterprise.
- Information about the frequency and consequences of the events included in the SNRA is at varying stages of maturity, with additional work required in some areas to ensure that event data can be appropriately compared. Where substantial additional research is warranted, events are discussed qualitatively and are not compared with other events.

- The SNRA methodology does not explicitly model the dynamic nature of some of the included hazards. For example, terrorists' evolving tactics in response to changes in defensive posture are not included.
- Experts consulted about psychological consequences emphasized caution in the application of the SNRA's measure of psychological distress, and stressed the need for additional research. The Department of Homeland Security and its partner organizations leveraged previously funded social and behavioral research to better understand how to anticipate, prepare for, counteract, and mitigate the effects of terrorist acts, natural disasters, and technological accidents. Additional research is required to further explore psychosocial factors that enable resilience in individuals, organizations, and communities and at the societal level.
- For national-level events where historic data was used as the basis of analysis, the risk from low-likelihood, high-consequence incidents may not be adequately captured. This is particularly true for technological/accidental hazards. Further study is needed to better characterize these risks at the national strategic level.

Impacts and Future Uses

The SNRA was executed in support of PPD-8 implementation and has served as an integral part of the development of the National Preparedness Goal, assisting in integrating and coordinating identification of the core capabilities and establishing a risk-informed foundation for the National Preparedness System. Participants mapped the core capabilities identified in the Goal to the events assessed in the SNRA to identify any additional core capabilities that may need to be included. In addition, the SNRA can be used to inform discussions on priorities for capability investment decisions. Finally, the SNRA results will be used to drive other preparedness priorities at the national level.

In addition, conducting a Strategic National Risk Assessment will support the National Preparedness System by providing a consolidated list of "national level events" for consideration and augmentation for Threat and Hazard Identification and Risk Assessment processes at multiple jurisdiction levels.

Conclusion

Although the development of the SNRA is an important first step, further analysis through the execution of regional- and community-level risk assessments will help communities better understand their risks and form a foundation for their own security and resilience. The Nation's preparedness is dependent on a whole-of-community understanding of risk and comprehensive consequences at and across all levels of government. In conjunction with Federal, state, local, tribal, and territorial partners, the SNRA will be expanded and enhanced and will ultimately serve as a unifying national risk profile to facilitate preparedness efforts.