Risk Frameworks for Climate

Natalie Prittinen and Ashley Stapp (Sandia National Laboratories)

Background/Objectives. The Risk Analytic Methods and Support (RAMS) team at Sandia National Laboratories (SNL) works to develop risk-based methodologies, tools, and capabilities for the USG in support of federal network and critical infrastructure protection. Through this work, the Cyber Risk Framework (CRF) was developed to assess the potential consequences of cyber attacks on critical infrastructure, particularly the 55 National Critical Functions (NCF). In 2021 and 2022, the RAMS team conducted an internal exercise to determine if the cyber analytic capability within the CRF could be applied to a climate change scenario. The objective of the exercise was to determine if the analytical resources currently available would be sufficient to address the climate scenario, identify gaps, and outline potential development areas.

Approach/Activities. The CRF process provides analysts with a principled, systematic, repeatable, pragmatic, and scalable risk analysis process for responding to decision support requests (DSR) from both public and private stakeholders, including federal, state, local, tribal, and territorial entities, as well as critical infrastructure operators. The five-step analytic process includes:

- *Triage*, in which the analyst determines stakeholder needs and requirements, characterizes key parameters of the DSR, and selects a decision support archetype to structure the analysis.
- *Define Scenario Space*, in which key dimensions of the cyber incident scenario (or scenarios) under consideration are specified for the purposes of bounding the analysis.
- *Perform Consequence Analysis*, in which either existing or new data sources and methods are used to provide consequence estimates.
- *Interpret Analytic Results*, in which raw outputs from consequence analysis are translated into meaningful and actionable outputs for decision makers.
- *Compile Final Assessment*, in which results are compiled and delivered in standardized format tailored to stakeholder requirements.

The internal exercise to “test” the CRF against a climate change request was designed around a fictional Executive Order (EO) that outlined a severe drought and related forest fire scenario in the western United States. The fictional EO called for a prioritized ranking of critical infrastructure most impacted by the drought and informed by potential direct and cascade-level impacts to the Water sector and related NCFs.

Results/Lessons Learned. The fictional EO required an analytical product within five days, so the RAMS team down selected the number of NCFs under consideration and restricted the analysis to two western states (California and Montana). The consequence analysis focused solely on human health and economic impacts, and a criticality logic was developed to “bin” scenarios into a tiered structure that included National Catastrophic, Regional Catastrophic, Locally Critical, and NCF Disruptive ratings. Final results of the exercise indicated that the CRF can successfully support a risk analysis of a climate change scenario at the same level of analysis as a cyber-attack scenario. The exercise identified several areas for future technical development, including time-dependent consequences (e.g., prolonged incident and inelastic responses), exploring cyclic approaches to criticality logics, and exploring cascading NCF dependency analysis.