SAND2023-02060C

# Systems Analysis at Sandia National Labs

## Risk Analytic Methods & Support (RAMS)

*Kevin Griffith*

April 2023

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

chnology & Engineering Solutions of Sandia, LLC,
s National Nuclear Security Administration under
contract DE-NA0003525.

# **BACKGROUND:** SYSTEMS ANALYSIS

- **Complex systems "…cannot be understood by studying parts in isolation.** The very essence of the system lies in the interaction between parts and the overall behavior that emerges from the interactions. The system must be analyzed as a whole." — Northwestern University

- **Systems analysis** is "…a systematic investigation of a real or planned system to determine the functions of the system and how they relate to each other and to any other system." Its objective is **"to provide information to … decision-makers that would sharpen their judgment and provide the basis for more informed choices."** — RAND Corporation

*"Our objective is understanding"*

# **BACKGROUND:** SYSTEMS ANALYSIS

- Provides data and information in a form that **supports improved decision-making**
- Is **honest** – i.e., does not seek a particular answer
- Is **objective** – i.e., does not skew toward a particular technology
- Relies on deep subject matter expertise, either among the analysts or in **close collaboration**
- Is **highly interwoven** with end-user and stakeholder interactions (can not be done well in an ivory tower)
  - The successful analyst should have some grit in their teeth
- Always **relies on some kind of model**, whether it is a simple mental model, a sophisticated HPC model, or anything in between
  - The trick is to determine the right fidelity to support the best possible decision, at reasonable cost, and in actionable time

*Help decision-makers make better decisions*

# **BACKGROUND:** SYSTEMS ANALYSIS

**Domain Expertise**

- Nuclear Deterrence
- Non-proliferation
- **Civil Cybersecurity**
- Machine Learning/AI
- Transportation Energy
- Climate & Resiliency
- Chem/Bio/Rad Threat
- Disaster Response
- Security Principles
- Human Resources/D&I

**Tools, Techniques, & Methods**

- **Problem Structuring**
- Expert Elicitation
- **Quant/Qualitative Analysis**
- Policy and Threat Assimilation
- Modeling and Simulation
- Experimental Wargaming
- Techno-Economic Analysis
- Data Analytics

**Cross-Domain Capabilities**

- Architectures
- Algorithms
- **Frameworks**
- Tabletop Exercises
- **RFI Response**
- **Risk Management**

*Help decision-makers make better decisions*

# **BACKGROUND:** SNL RISK SUPPORT

**SNL has historically developed a multitude of tools and models to support risk prioritization, leveraging expertise in all hazards analysis, nuclear weapon research, and systems analysis to support risk needs across federal networks and critical infrastructure.**

SNL has leveraged the lab's technical understanding of risk from other disciplines, including decades of nuclear weapon research, to provide rigor and analysis to assessing risk in the nation's supply chains and critical infrastructure.

SNL supports the Department of Homeland Security's (DHS) role in providing cybersecurity and critical infrastructure  risk management to the federal government by creating implementable solutions for risk assessments.

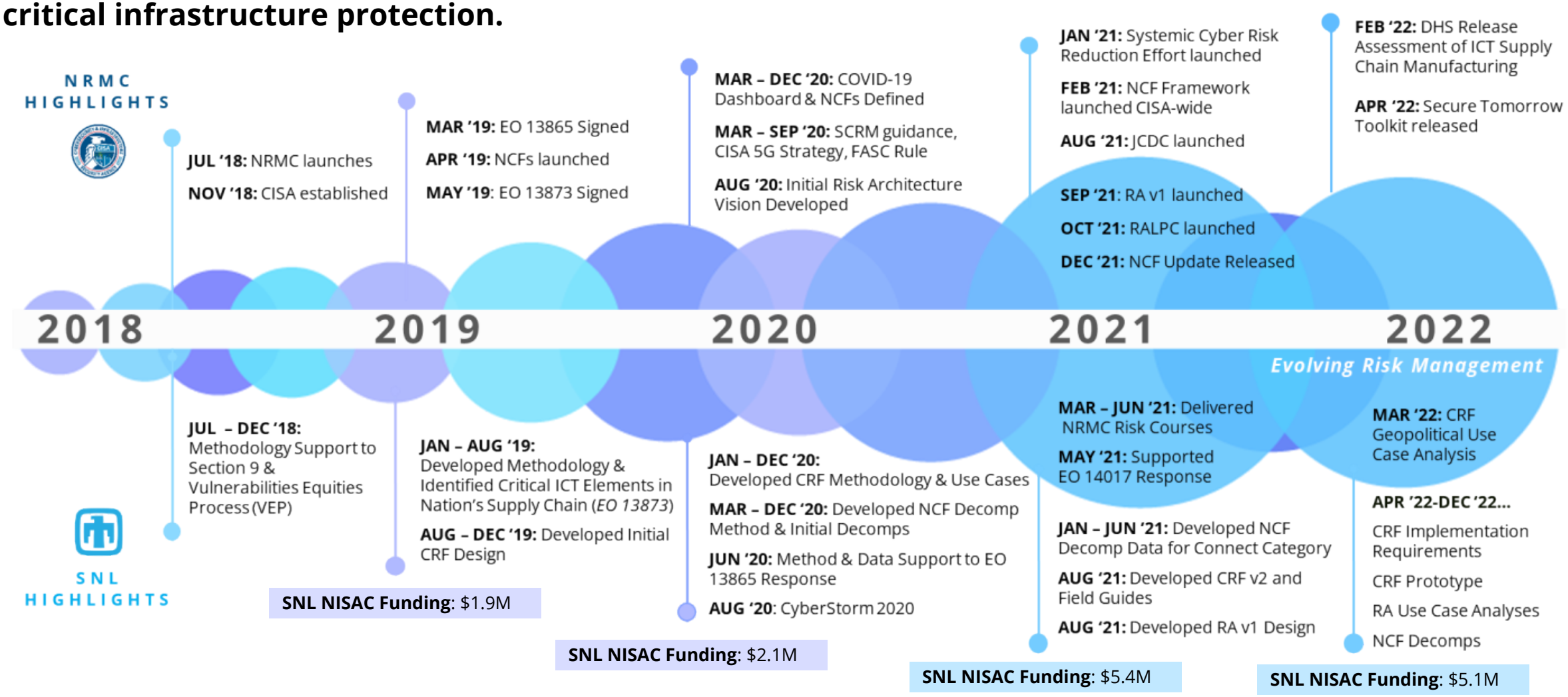
SNL is engaged with stakeholders on both the policy and technical side to consider how shifts in legislation and technological development require expanding and updating of existing tools designed to mitigate risk.

SNL has supported the NISAC program since 2004.  Previous work focused on developing a multitude of tools and models to support analysis of disruptive impacts on critical infrastructure sectors, through SNL support to DHS's Office of Cyber and Infrastructure Analysis (OCIA).

Through the establishment of the National Risk Management Center (NRMC) and the evolution of NISAC, SNL's support has evolved to focus on providing risk frameworks, design principles, and analysis capabilities to assess interdependent risks across National Critical Functions and critical infrastructure.

# **BACKGROUND:** EVOLVING NRMC PORTFOLIO SUPPORT

**Since NRMC's establishment, SNL's Risk Analytic Methods and Support (RAMS) team has expanded their development of risk-based methodologies, tools, and capabilities in support of federal network and critical infrastructure protection.**



# BACKGROUND: CURRENT SNL NRMC PORTFOLIO

**The Risk Analytic Methods and Support (RAMS) portfolio performs work to develop risk-based methodologies, tools, and capabilities for USG in support of federal network and critical infrastructure protection.**

**BOND RATINGS**: Explore the feasibility of using bond rating approaches to characterize systematic risk through tracking quantitative risk proxies and structured SME engagement.

**DIGITAL TRANSFORMATION OF RISK:** Explore cloud optimization opportunities as it relates to the development, sustainability, and accessibility of STAR capabilities.

**ADVERSARY-DRIVEN SCENARIOS:** Explore gaps in adversary behavior analysis focused on likelihood modeling methodologies and their applicability to critical infrastructure and cyber scenario risk analysis.

**SUITE OF TOOLS FOR THE ANALYSIS OF RISK (STAR):** Create a scalable framework that leverages National Critical Function (NCF) dependencies, data structures, & analytic capabilities to provide critical decision support and risk analysis.

**EMERGENCY RESPONSE PRIORITIZATION :** Develop a risk framework that would enable emergency managers to prioritize pieces of infrastructure that are most at risk during a natural hazard event.

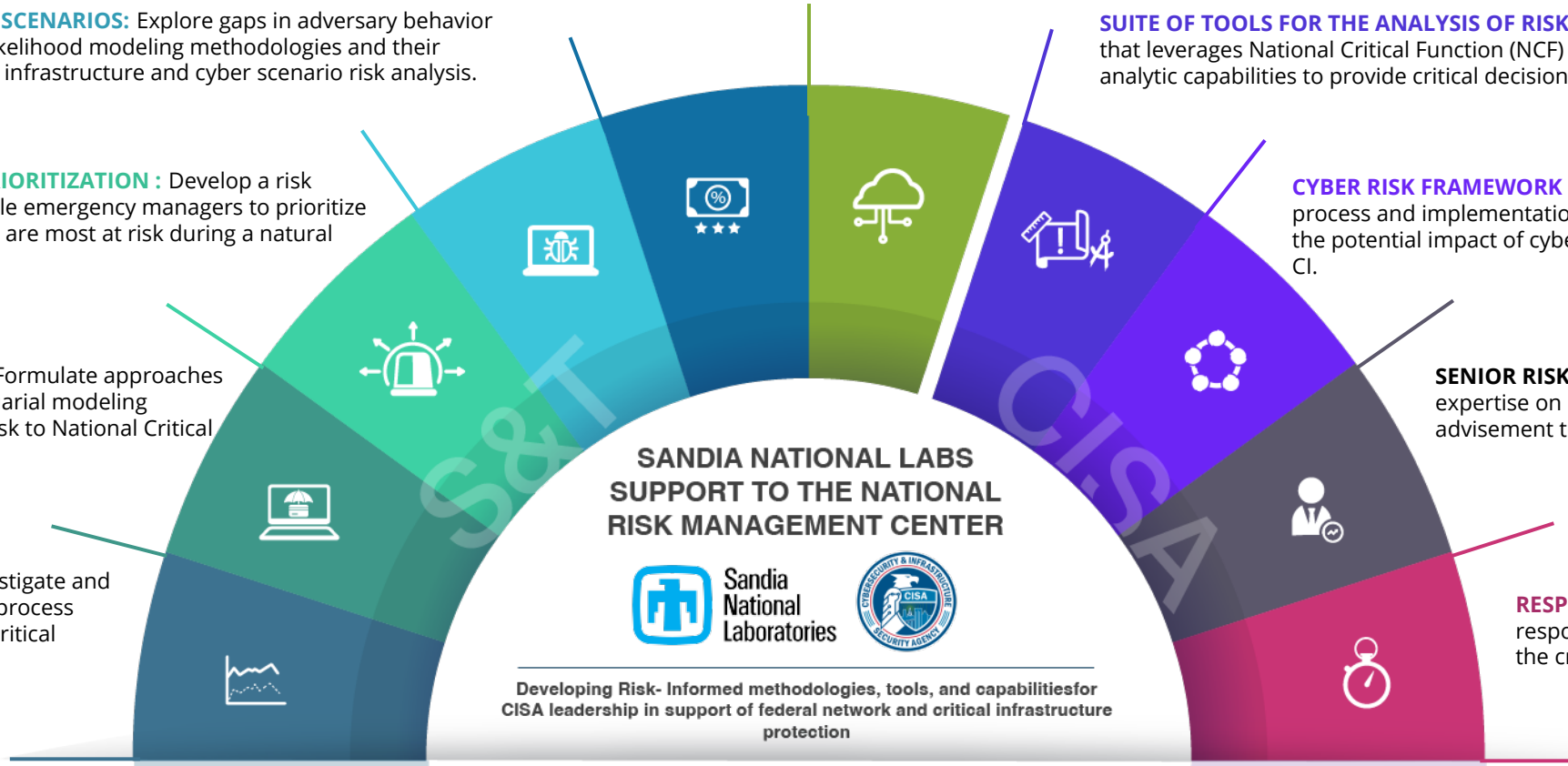
**CYBER RISK FRAMEWORK (CRF):** Develop a risk analytic process and implementation that allows for the assessment of the potential impact of cyber attacks on federal networks and CI.

**ACTUARIAL APPROACHES:** Formulate approaches that allow application of actuarial modeling concepts to the analysis of risk to National Critical Functions (NCFs).

**SENIOR RISK ADVISOR:** Provide subject matter expertise on STAR development and targeted advisement to NRMC leadership.

**PREDICTION MARKETS:** Investigate and develop a prediction market process tailored to NRMC's focus on critical infrastructure risk.

**RESPONSIVE TASKING:** Provide responsive risk analysis support across the critical infrastructure risk landscape.



# CAPABILITY SPOTLIGHT: CYBER RISK FRAMEWORK (CRF)

**The Cyber Risk Framework (CRF) is a risk analytic process under development by Sandia National Laboratories for CISA's National Risk Management Center in their assessment of the potential impacts of cyber-attacks on federal networks and critical infrastructure (CI).**

**GOAL:** Provide analysts with a principled, systematic, repeatable, pragmatic, and scalable approach to consequence analysis that draws on established risk methods and can incorporate diverse analytic tools, data sources, and modeling capabilities.

**The Cyber Risk Framework (CRF) provides analytic value through:**

- Organizing and standardizing consequence assessment methodologies across the CI space, building upon existing risk analytic principles and practices.
- Supporting the development and maintenance of stakeholder-relevant metrics.
- Providing a flexible approach responsive to given changes in the technology, threat, and infrastructure environment.
- Enhancing NRMC's mission support of CISA's role as the Nation's Risk Reducer.

**The CRF is built on a set of core analytic concepts:**

- **Reusable methodologies:** A core set of methods and approaches built around patterns in request for analysis can support a range of standard request types.
- **Scalability.** The CRF process should be applicable at any level of required analytical sophistication; analytical methods and approaches may change, but the fundamental approach is consistent.
- **Knowledge management.** The Scenario Results Library will catalog existing analyses, both from previous requests and prospective studies, providing analysts with "pre-baked" results that can be leveraged in support of new requests.

# CAPABILITY SPOTLIGHT: CYBER RISK FRAMEWORK (CRF)

**The five-part process provides a structured approach to problem framing, scenario generation, consequence estimation, and development of stakeholder-appropriate products and decision aids.**

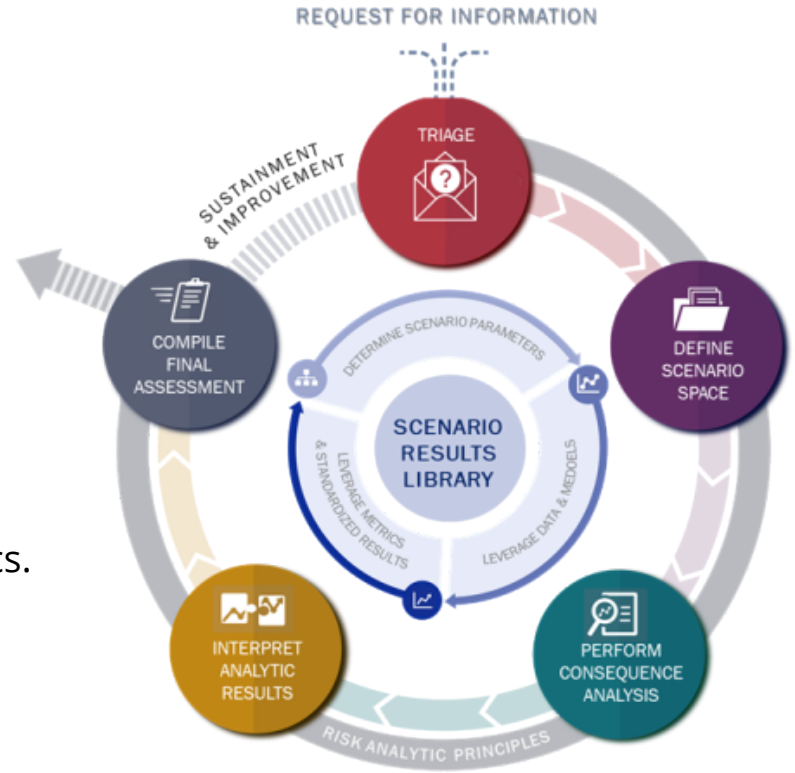
**Triage based on Request for Information:**
Analysts determine stakeholder needs and requirements and characterize key parameters of the RFI to structure the analysis.

**Define Scenario Space:**
Analysts specify key dimensions of the cyber incident scenario (or scenarios) under consideration for purposes of bounding analysis.

**Perform Consequence Analysis:**
Analysts leverage existing data sources and methods or, if necessary, generate new analysis to estimate impacts on stakeholder-relevant metrics.

**Interpret Analytic Results:**
Analysts translate raw outputs from consequence analysis into meaningful and actionable outputs for decisionmakers.

**Compile Final Assessment:**
Analysts compile final results into standardized formats tailored to stakeholder requirements.




**CYBER RISK FRAMEWORK**

# CAPABILITY SPOTLIGHT: CRF APPLICATION

*EO 13865 Response Assessment*

**SNL leveraged the Cyber Risk Framework to develop a rapid response assessment in support of NRMC's response to Executive Order 13865 "Coordinating National Resilience to Electromagnetic Pulses."**

**NRMC received the request for information (RFI) from the Executive Branch through EO 13865.**

SNL applied a series of categorizing filters to scope the Request for Information**:**

- ❑ **Intended Audience:** Executive Branch, NSC
- ❑ **Intended Output: 1:** Criticality Assessment Methodology for EMP-vulnerable NCFs
- ❑ **Intended Output 2:** Tiered list of associated critical systems, networks, and assets.

**Analysts triaged the RFI based on one-week time frame to respond and select critical assets.**

To form an approach, the team leveraged previously developed methodologies and tools:

- ❑ Level 0 Hazards Analysis
- ❑ ICT Elements List Framework (EO 13873)
- ❑ Criticality Assessment Logic (EO 13873)
- ❑ Data-Driven Decomposition Methodologies

**Analysts then scoped the response based on Comms and Energy sector NCFs and critical components.**

SNL then scoped NCFs for analysis in consultation with NRMC, to identify critical Systems, Networks, and Assets (SN&As).

**Communications Sector NCFs**

- ❑ Operate Core Network
- ❑ Provide Cable Access Network Services
- ❑ Provide Internet Based Content, Information, and Communications Services
- ❑ Provide Internet Routing, Access, and Connection Services
- ❑ Provide Positioning, Navigation, and Timing Services
- ❑ Provide Radio Broadcast Access Network Services
- ❑ Provide Satellite Access Network Services
- ❑ Provide Wireless Access Network Services
- ❑ Provide Wireline Access Network Services

**Energy Sector and Other NCFs**

- ❑ Distribute Electricity
- ❑ Transmit Electricity
- ❑ Generate Electricity
- ❑ Maintain Access to Medical Records
- ❑ Manage Wastewater
- ❑ Prepare for and Manage Emergencies
- ❑ Provide Medical Care
- ❑ Provide Public Safety
- ❑ Supply Water

*Notional Results*

# CAPABILITY SPOTLIGHT: CRF APPLICATION

*EO 13865 Response Assessment*

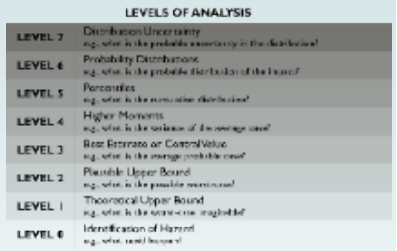
**SNL leveraged the Cyber Risk Framework to develop a rapid response assessment in support of NRMC's response to Executive Order 13865 "Coordinating National Resilience to Electromagnetic Pulses."**

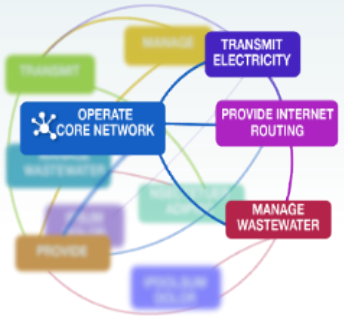
PERFORM CONSEQUENCE ANALYSIS

**Analysts conducted a Level 0 Hazard Analysis to determine consequence parameters and interdependencies.**

SNL performed a **Level 0 Analysis** to determine known and potential impacts to national security, the economy, and public health, and of an EMP event on in-scope NCFs.

This analysis highlights NCF interdependencies and ICT pinch points.




INTERPRET ANALYTIC RESULTS

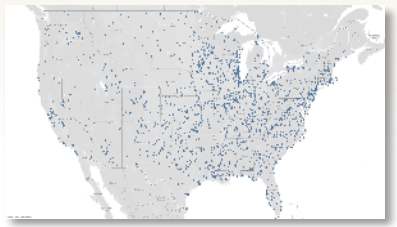
**Analysts developed Criticality Logic to determine criticality across NCF & ICT asset pairs.**

SNL applied the developed Criticality Assessment Logic (CAL) to tier asset-NCF pairs based on defined consequence criteria in previous step.

The team identified additional data-driven approaches that could contextualize criticality data.

**CAL Methodology**

**Data-Driven: Cell-Tower Distribution**



COMPILE FINAL ASSESSMENT

**Analysts compiled final results, data driven methods and determinations into final assessment.**

SNL aggregated all developed methodological inputs and recommendations for future assessments into a defined format for NRMC.

- ❑ Criticality Assessment Methodology
- ❑ Tiered list of SN&As
- ❑ Methodological assumptions & limitations
- ❑ Recommendations for Application
- ❑ Visual Aids


*Notional Results*

# CAPABILITY SPOTLIGHT: CRF APPLICATION

*FY22 USE CASES*

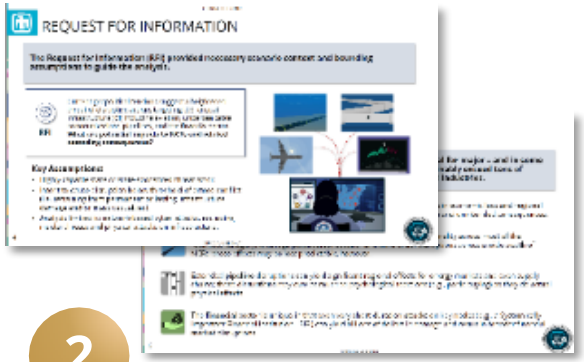
**As part of the CRF Applications focus in FY22, SNL demonstrated CRF utility through collaborative use cases. Use case analyses revealed potential inputs to identified STAR capabilities and additional areas of data generation.**

## FY22 CRF APPLICATIONS USE CASES


1

***Deliberative Use Case:***
**Water-ICS Cyber Scenarios**

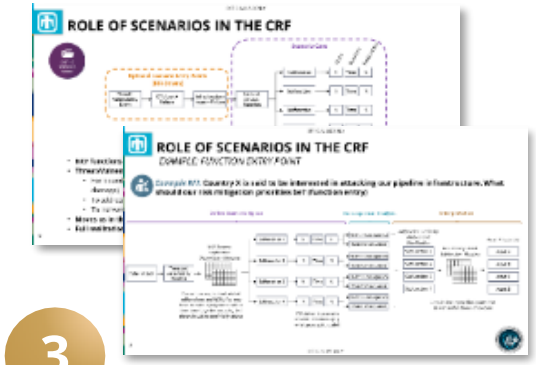
The Water-ICS use case leveraged scenario data on potential cyber compromises of Industrial Control Systems (ICS) used in water treatment and distribution infrastructure.




2

***Responsive Use Case:***
**Geopolitical Incident Impact on CI**

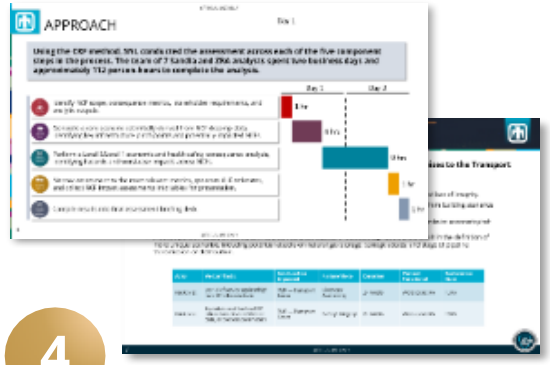
The geopolitical use case explored potential impacts on critical infrastructure and NCFs if interrupted by a geopolitical event or incident.




3

***Deliberative Use Case:***
**Food-Ag Production Disruption**

Leveraging a set of existing NCF data, SNL developed a deliberative analytic use case addressing cross-sector cyber threats to agriculture and communications-related NCFs.




4

***Responsive Use Case:***
**48-Hour Pipeline Disruption Response**

SNL conducted a responsive assessment on a hypothetical pipeline incident across each of the five component steps in the process.

# CAPABILITY SPOTLIGHT: CRF APPLICATION

*GEOPOLITICAL USE CASE*

**Using the CRF method, SNL found across all four categories of critical infrastructure the potential for major – and in some cases critical – NCF disruptions.**

RFI

Current geopolitical tensions suggest a heightened threat of disruptive actions targeting U.S. critical infrastructure (CI) including aviation, undersea cable communications, pipelines and the financial sector. **What are potential impacts to NCFs and related cascading consequences?**

*Example Question*

**Aviation** is one of the "safest" targets, offering potential billions of dollars in economic loss and regional supply chain disruptions, while limiting permanent infrastructure damage and unintended consequences.

**Undersea cable** attacks offer opportunity to disrupt regional NCF functionality across most of the "Connect" category, with high potential for second and third orders disruptions across a wide swath of NCFs; these effects may be less predictable, however.

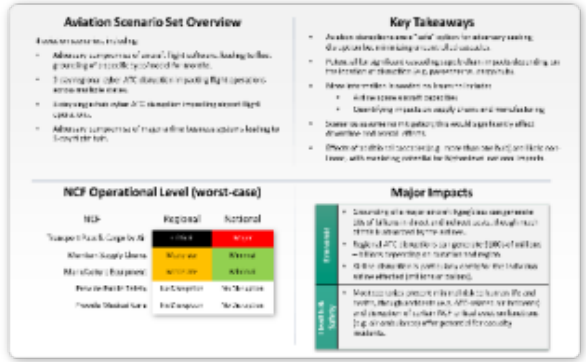
Extended **pipeline** disruptions can yield significant regional effects for energy markets and even supply chains; these disruptions may owe as much to psychological reactions (e.g., panic buying) as they do actual physical effects.

The **financial** sector is unique in that even very short-duration attacks on key nodes (e.g., a Systemically Important Financial Institution - SIFI) can yield billions of dollars in damage and result in broader financial market disruptions.

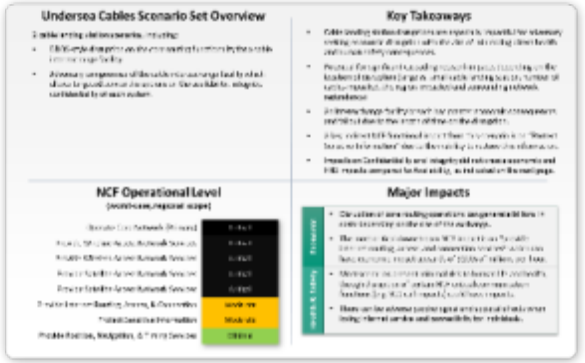
*Notional Results*

*Analytic Structure*

AVIATION




UNDERSEA CABLES




*Notional Results*

# CAPABILITY SPOTLIGHT: CRF APPLICATION

*FOOD-AGRICULTURE CYBER DISRUPTION USE CASE*

**Using the CRF method, SNL found the potential for appreciable impacts across growing, harvesting, distribution and production phases of NCFs, but effects were highly dependent on the ag sector under consideration**

*Example Question*

**RFI**

Large-scale agricultural operations increasingly rely on wirelessly networked operational technologies and industrial control systems for monitoring and management of essential functions. **What are the possible consequences of such an attack, including potential downstream impacts across the growing, harvesting, processing, and distribution phases of food/ag functions?**

- **SNL leveraged simple threat assumptions to frame the scenario, including:**
  - Unspecified actor attempting to cause disruption to precision agriculture functions.
  - Compromise of wireless access network supporting IT/OT used in management of agricultural operations.
  - Intent to undermine data integrity.

- **Available NCF decomposition dependency data was used to identify key sub-function touchpoints in 47 (“Provide Agricultural Products & Services”) and 48 (“Provide Food Products & Services”), as well as related intra-and inter-NCF dependencies.**

**NCF Operational Level (Region 8/HRS)**

| National Critical Function | Regional Impact | National Impact |
|---|---|---|
| NCF8 Provide Wireless Access Network Services | Moderate | Minimal |
| NCF47 Produce & Provide Agricultural Products & Services | Moderate | Minimal / Moderate* |
| NCF48 Produce & Provide Human & Animal Food Products and Services | Moderate | Minimal / Moderate* |

*National-level NCF impact dependent on supply-demand elasticity, including available yield of non-impacted crop, product substitutability, and import availability.

**Major Impacts (Region 8/HRS)**

**Economic**

- Potential yield impact of 5-70%, varying with nature of the compromise and effecting those HRS farms dependent on technology (est. 20-25%).
- Potential economic losses in the 10s to 100s of millions of dollars, including taxpayer-subsidized insurance payouts.
- Likely minimal impact to national food production and supply chains given overall yield, elastic demand, and substitution options.

**Health**

- Potential health consequences from agricultural runoff and excess pesticides if compromise results in over-distribution of these inputs.

*Notional Results*

# **CONCLUSION:** SYSTEMS ANALYSIS

## Should…

- Keep an open mind
- Work closely with client to scope the question, develop meaningful metrics, and sketch out the form of the results so that they will be actionable
- Question and clarify all terminology and assumptions
- Handle uncertainties and variability
- Clearly communicate assumptions
- **Improve the intuition of the decision-maker**

## Should not…

- Attempt to take the place of the decision-maker or tell them what to do
- Blindly attempt to answer the question without first exploring assumptions and understanding the decision
- Seek only to prove (and not also to disprove) a hypothesis
- Generate piles of data and/or paper and assume that is sufficient
- Overwhelm the decision-maker with complexity and sum up with “trust us, this is the right answer”

# **CONCLUSION:** SYSTEMS ANALYSIS

Thank you!