Electric Infrastructure Protection (EPRO®) Handbook III

Cross-Sector Coordination and Communications in Black Sky Events
EPRO Handbook

First Edition – June 25, 2018
First Printing – June 25, 2018
Copyright © 2018 by the Electric Infrastructure Security (EIS) Council

ISBN 978-0-9971659-3-7

Editor in Chief and Author of Executive Summary and Chapter I
Dr. Paul Stockton, Managing Director, Sonecon LLC; Former U.S. Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs

Author of Chapter II
Dr. Neil Siegel, Chief Engineer, EIS Council; The IBM Professor of Engineering Management, University of Southern California; Retired Sector Vice-President & Chief Technology Officer, Northrop Grumman. Dr. Siegel gratefully acknowledges the contributions of Bran Ferren and his company, Applied Minds, LLC, to the materials in this chapter.

Contributing Editors
Avi Schnurr, CEO and President, EIS Council
Dr. Chris Beck, Vice President for Policy and Strategic Initiatives, EIS Council
John Organek, Director, Program Planning and Operational Architecture, EIS Council
Rob Denaburg, Senior Analyst, Sonecon LLC
Joey Schnurr, Technical Director – Infrastructure Simulation, EIS Council
Scott Blevins, Communications Sector Coordinator, EIS Council

Acknowledgments

Development and production of this Handbook relied on the insights, consultations, and review from many individuals and organizations. Although they cannot all be acknowledged here, the editors and publisher wish to express their deepest appreciation to the many contributors to this Handbook, worldwide.

Special thanks to PJM Interconnection, LLC and its leadership team, including: Andy Ott, President and CEO; Thomas O’Brien, Senior Vice President and Chief Information Officer; and Johnathon Monken, Senior Director, System Resiliency and Strategic Coordination. This Handbook was made possible by their many contributions.

Published by
The Electric Infrastructure Security (EIS) Council

Image Copyright Disclaimer

All images included in the Handbook are entirely the work of their respective authors, and their use does not imply the endorsement of EIS Council, the Handbook, or any of its related products by the authors. Images containing U.S. Government personnel or property do not imply the endorsement of EIS Council by the United States Government.

All images are unaltered, and free to use either as part of the Public Domain, or with appropriate attribution and credit given to the respective authors.
EPRO® Handbook III
Cross-Sector Coordination and Communications in Black Sky Events
# Table of Contents

EXECUTIVE SUMMARY ................................................................. 11

INTRODUCTION ............................................................................. 13
   A. Black Sky Events: Maria and Beyond ........................................ 16
   B. Black Sky Hazards: Objectives, Key Questions, and Integrated, Systems Engineering-Based Planning ............................................ 20

CROSS-SECTOR COORDINATION CHALLENGES, AND STRATEGIES AND STRUCTURES FOR COLLABORATION .......... 25

BLACK SKY EMERGENCY COMMUNICATIONS AND COORDINATION SYSTEM (BSX) ......................................................... 32
   Key findings and recommendations .............................................. 34

THE WAY FORWARD: BUILDING A SUITE OF BLACK SKY RESPONSE TOOLS AND TECHNOLOGIES ........................................... 37
   Essential BSX System Functions .................................................. 38

CHAPTER ONE: SUSTAINING AND RESTORING CRITICAL INFRASTRUCTURE IN BLACK SKY EVENTS .............................. 41

INTRODUCTION ............................................................................... 43

I. CHAPTER OVERVIEW ............................................................... 45

II. CROSS-SECTOR RESILIENCE: CHALLENGES AND IMPERATIVES FOR PROGRESS ......................................................... 61
   A. Emerging Infrastructure Fragilities .......................................... 63
   B. Complex Cross-Sector Interdependencies: The Emerging System of Systems ................................................................. 73
   C. Threats to Cross-Sector Resilience: The Strategic Challenge ........ 87

III. BLACK SKY PRIORITIZATION: STRATEGIES TO IDENTIFY AND STRENGTHEN CRITICAL FACILITIES, SUPPLY CHAINS, AND ASSETS ................................................................. 112

IV. INFRASTRUCTURE OWNERS AND OPERATORS: CROSS-SECTOR PLANNING AND COORDINATION FOR BLACK SKY RESILIENCE ................................................................. 123
The ELECTRIC INFRASTRUCTURE PROTECTION (EPRO®) HANDBOOK® SERIES

A source of peer-reviewed analysis and recommendations to help infrastructure owners and operators, government agencies, and non-governmental organizations bolster resilience against Black Sky hazards.
INTRODUCTION

The electrification of our planet has become the foundation for the technological progress that is shaping the 21st century. As electricity has become more widely available and reliable, it has transformed modern society and made possible today’s unprecedented network of interconnected infrastructure systems, from food and water distribution to the internet and beyond. The “electrification of everything” has also enabled the rise of today’s megacities and the continued growth of the global economy.

However, this tightening web of connectivity also makes infrastructure sectors extraordinarily dependent on each other and vulnerable to cascading failures. “Black Sky” events – subcontinent scale power outages lasting a month or more – represent a particularly serious risk. A broad array of natural and manmade hazards could cause such catastrophic blackouts, including extreme earthquakes, attacks by
Electromagnetic Pulse (EMP) weapons, and coordinated cyber and physical attacks against critical grid components.

On a smaller geographic scale, the power outage that Hurricane Maria inflicted on Puerto Rico in September 2017 exemplifies how Black Sky outages will create cascading failures across a broad array of electricity-dependent infrastructure. Water utilities, communications systems, transportation infrastructure, and many other resources and services rapidly broke down when they lost power.

Deepening cross-sector interdependencies will also magnify mutually-reinforcing failures between critical systems, with novel and potentially catastrophic effects in Black Sky events. A prime example: in order to restore power in the event of a catastrophic blackout, electric companies rely on communications, transportation, and other infrastructure systems to support repair operations and sustain their personnel. But those same infrastructure systems depend on electricity to function. With nearly all infrastructures now hyperconnected, no single system – including the electricity subsector – can carry out restoration operations without at least minimal functionality of many other sectors. As a result, Black Sky outages will jeopardize societal continuity unless the United States and partner nations strengthen cross-sector resilience.

This Handbook offers new approaches to bolster such resilience. The Handbook provides recommendations on how infrastructure owners and operators and their partners in government and non-governmental organizations (NGOs) can build on – and rapidly accelerate – progress in creating multi-sector preparedness plans, capabilities for mutual support, mechanisms for coordination, and survivable, widely-deployed systems for communications and decision support.

Preparedness for Black Sky events will still require that, within each infrastructure sector, system owners and operators harden their own assets against manmade and natural hazards. Those sector-specific initiatives are vital and should be scaled up for catastrophes worse than ever experienced in the United States.
However, given the deepening interdependencies between sectors, and the intensifying risks of cascading and mutually-reinforcing failures, it is also essential to take two further steps:

1. **Develop Cross-Sector Plans and Coordination Mechanisms:**
   Infrastructure owners and operators will need to pre-plan with government agencies and NGOs for two key lines of effort in Black Sky events: 1) sustain service to hospitals, key military bases, and other vital facilities to keep them functioning; and 2) rapidly restore critical infrastructure services where outages occur. Mechanisms for real-time coordination of these Black Sky response operations will also be essential.

2. **Create and Deploy Multi-Sector Systems for Emergency Communications and Decision Support:**
   Cross-sector coordination will be impossible unless infrastructure operators and their government and NGO counterparts have survivable, widely-distributed communications and decision support systems (including hardware and software) to establish situational awareness in severely disrupted environments and help guide and prioritize response operations.

The chapters that follow provide recommendations to meet these requirements. They also examine the risks that rising interdependencies create for critical infrastructure resilience, and analyze how recent private sector and government initiatives (including the issuance of the Power Outage Incident Annex)\(^1\) can be leveraged to build preparedness for Black Sky events.

---

A. Black Sky Events: Maria and Beyond

On September 20, 2017, Hurricane Maria inflicted Black Sky levels of disruption on Puerto Rico. Power outages extended for more than a month over most of the Commonwealth, creating cascading and mutually-reinforcing failures across all critical infrastructure sectors.

However, the area devastated by Maria was much smaller than would be disrupted by EMP attacks or other Black Sky hazard in the continental United States. And, particularly critical, the largest cities of Puerto Rico are just a few percent of the size of typical U.S. megacities, which will pose additional challenges for both access into cities and the distribution of critical supplies within them.

Maria is also atypical of Black Sky events in another respect: the hurricane left the mainland’s vast disaster response system untouched. A Black Sky event spanning multiple U.S. regions will disrupt the infrastructure on which that response system depends. It will also create immense challenges for prioritizing the sustainment and restoration of critical services, as well as the resupply of fuel for emergency generators and other essential resources.

Nevertheless, while occurring on a smaller scale, Puerto Rico’s tragic experience with Maria offers useful insights into the cross-sector failures that Black Sky events will create. Those failures also help illuminate the requirements for strengthening infrastructure resilience that provide the focus of this volume.

Hurricane Maria exemplifies the way in which Black Sky hazards will cause interdependent sectors to collapse at the same time. Due to direct damage from wind, flooding, and other weather effects, electricity transmission and distribution systems, cellphone towers, and other infrastructure quickly failed. So, too, did the water systems and other sectors dependent on the flow of electricity. Even the emergency managers leading the response to Maria were forced to evacuate the buildings where they had taken shelter. “Everything collapsed,” said Héctor Pesquera, the Puerto Rico governor’s director of safety.
and public protection. “Everything collapsed simultaneously.” Future Black Sky events in the continental United States will create such cross-sector devastation on a much larger geographic scale.

Maria also highlights how cross-sector failures will impede the restoration of service critical to saving and sustaining lives. For example, breakdowns in the oil and natural gas (ONG) subsector, including in the distribution of diesel and other liquid fuels, produced many such delays. Hundreds of containers of perishable food and medicine were stuck in ports because trucking systems lacked the fuel to operate. Diesel for emergency power generators at hospitals, supermarkets, and other facilities quickly ran out. Due to the lack of electricity for pumps and other key fuel resupply systems, these vital facilities could not be replenished for weeks – even with extensive help from the US mainland.

As a primary lesson-learned, Maria helps illustrate the critical need to build both organizational / structural mechanisms and hardware support tooling that can provide for cross-sector coordination against much larger Black Sky events. Especially important:

*Infrastructure owners and operators, government agencies, and non-governmental organizations will require collaborative decision-making mechanisms.*

---


Maria inflicted such extensive damage on Puerto Rico’s infrastructure that it was extraordinarily difficult to sustain or restore essential services. Doing so in multi-region Black Sky events will present still greater challenges. A growing number of infrastructure owners and operators are building Black Sky playbooks to help meet these challenges and are specifying the support they will need from other sectors to help sustain critical functions and prioritize restoration operations.

However, future Black Sky events will also require cross-sector collaboration on a nationwide scale. Given the overwhelming destruction that such events will create, as well as the scarcity of resources to fix or replace key infrastructure components, difficult decisions will need to be made about the order in which specific sustainment and restoration operations should go forward. And with the multi-region supply chains that sustain all infrastructure, resource, and service sectors, even local infrastructure restoration and population sustainment efforts will require national scale coordination.

Individual infrastructure owners and operators are best positioned to determine their own priorities for assistance. However, in Black Sky events, industry leaders will need to help integrate sustainment and restoration priorities across virtually all sectors to inform collaborative response operations throughout major portions of the United States. Doing so will require: 1) the widely interconnected emergency communications, situational awareness, and decision support mechanisms necessary to support prioritized, multi-sector sustainment and restoration; and 2) collaborative bodies in which industry, government, and NGO leaders from all sectors essential for responding to Black Sky events can set operational priorities and help ensure their implementation.

As an integral part of such collaborative bodies, deep engagement between industry leaders and their government counterparts will be necessary to effectively integrate cross-sector operations across all aspects of Federal, state, local, tribal, and territorial (SLTT) Black Sky response and recovery efforts. Close collaboration will also be needed with the NGOs that will provide mass care and other essential services in Black Sky events.

The National Response Framework (NRF) provides the ideal foundation on which to build such public-private collaboration. Moreover, in the midst of the
response to Maria, the Federal Emergency Management Agency (FEMA), DHS’ National Protection and Programs Directorate, other Federal agencies, and their private sector partners developed innovative mechanisms to strengthen cross-sector situational awareness and facilitate mutual support. Chapter I examines these “on the fly” initiatives and considers how they might be institutionalized and scaled up for Black Sky events. Nevertheless, enormous gaps remain in the NRF for guiding cross-sector support. This volume proposes new strategies and collaborative structures to fill them.

*Survivable communication and coordination systems are of core importance for infrastructure sustainment and restoration.*

Brock Long, Administrator of the Federal Emergency Management Agency (FEMA), notes that Hurricane Maria’s near-total disruption of communications in Puerto Rico has implications for disaster preparedness for the United States as a whole. He emphasizes that “we basically just went through a complete and total communication blackout for an island and it creates a lot of panic, a lot of misunderstanding, a lot of misinformation, and that was incredibly frustrating. So I think we have a lot of work to do for survivable [communications].” In particular, he argues that because “we become more and more vulnerable every day as we go to digital networks,” having communications systems “designed to handle all hazards” is of paramount importance to prevent public panic and manage response operations.

None of the cross-sector collaboration essential for Black Sky events will go forward unless a survivable, widely-distributed communications and coordination system is available to enable and support real time operations,

---

decision-making and prioritization. Development of a prototype of such a system – the Black Sky Emergency Communications and Coordination System (BSX™) – is already underway, along with the situational awareness tool and the artificial intelligence (AI)-enabled decision-support model that BSX is designed to host. This Handbook examines the key features of BSX™, the user-based analysis that underlies its design, and how the system can best evolve to meet the requirements of Black Sky events.

B. Black Sky Hazards: Objectives, Key Questions, and Integrated, Systems Engineering-Based Planning

Objectives

1. Building preparedness for Black Sky events will require accelerated efforts in three realms:
2. Accurately model the increasing interdependence of critical infrastructure sectors
3. Define and invest in essential resilience resources and create the cross-sector plans and capabilities needed to:
   • Support multi-sector sustainment and restoration for vital facilities and functions
   • Sustain the affected population, especially by enabling shelter in place strategies as restoration proceeds
4. Deploy the survivable communication and coordination systems essential for both intra-sector and cross-sector operations.

If such objectives are to be met for both natural and manmade hazards, efforts must take into account the risk that adversaries will:

A) Design their attacks to exploit sector interdependencies, maximizing the cascading and mutually-reinforcing infrastructure failures that they create.
B) Seek to disrupt the cross-sector operations we perform to sustain and restore critical services once the attack is underway, and cripple the communications and coordination systems on which those operations depend.

**Fundamental questions raised by Black Sky hazards**

As in any enterprise, the first step must always be to ask – and answer – critical underlying questions that point toward the efforts that will follow. While seemingly simple, explicitly putting such basic questions on the table can be enormously helpful in guiding planning and strategizing efforts.

This is particularly true of Black Sky hazards, where the underlying question can help decision makers understand the societal consequences of the question and the implications of the answer.

For Black Sky events, this becomes a fundamental, existential question:

> “Do the United States and allied nations wish to be prepared to survive Black Sky outages?”

And, if this question is to have practical meaning, it must be accompanied by a close corollary:

> “Should we challenge ourselves to develop cost effective approaches to address this need?”

**Integrated, Systems-Engineering Based Planning for Black Sky hazards**

If the answers to these two interrelated questions are both “yes,” and if such answers are to be meaningful, there are several implications for the work that lies ahead. In particular, carefully coordinated, integrated, sector-by-sector resilience investment and planning to address Black Sky scenarios will be essential. How can such integrated, multi-sector planning be framed?
Rigorous, systems engineering-based planning provides an excellent template for such a process, ensuring that each segment of any enterprise focuses their efforts on a mission compatible with the overall goal. Each segment – in this case, individual public or private sector critical infrastructure and emergency management stakeholders - must then define their internal and external requirements for accomplishing this goal.

For societal infrastructures and other key resource and service categories, this may be characterized as responses to the following questions:

1. **Black Sky sector missions**  
   In such catastrophic events, what essential services, resources, or other support should each sector be prepared to provide to partner sectors and the populations they serve?

2. **Black Sky sector-specific “internal” requirements**  
   What cost-effective operational planning and specific resilience measures will be needed by each infrastructure sector to strengthen its own resilience against Black Sky hazards?

3. **Black Sky sector-specific “external” requirements for assistance**  
   What support, resources, or new externally-controlled policy frameworks will each sector require from its cross-sector partners and other resilience stakeholders to make its own efforts meaningful and effective?

**Black Sky resources**

A growing number of infrastructure owners and operators and their resilience partners are now addressing these issues, especially in the energy, water and wastewater, and emergency management sectors. Their development of Black Sky Playbooks and related efforts has been supported by the EPRO SECTOR Project, the EARTH EX and Black Sky Exercise Project, and by EPRO Handbooks I and II. Each Handbook addressed a specific Black Sky challenge:

- **EPRO Handbook I**  
  This initial Handbook recommended an array of options to scale up infrastructure protection and power restoration operations to help
utilities and their partners reduce the scope and duration of outages that severe hazards can cause.

- **EPRO Handbook II - Volume I**
  
  Volume I of this follow-on Handbook examined opportunities to strengthen the resilience of fuel supplies for power generation in Black Sky events, especially natural gas. The Handbook highlighted the growing interdependencies between the energy subsectors that magnify the potential for cascading, mutually-reinforcing failures and increase the risk of catastrophic power outages.

- **EPRO Handbook II - Volume II**
  
  Volume II of this follow-on Handbook provided recommendations on strengthening the resilience of the water and wastewater sector against Black Sky outages. The Handbook examines how the ability of water and wastewater systems to sustain emergency operations in a Black Sky event will offer a particularly valuable means to avert catastrophic threats to societal continuity and human life.

**The challenge ahead: Key questions for multi-sector collaboration, communication, and coordination in Black Sky events**

Black Sky planning is now beginning to move forward in multiple sectors. The next, urgent step is to begin planning for the coordination frameworks and tools essential to tie all such efforts together – both before an event, and during the complex response phases after it occurs. As a first step, such efforts must respond to several fundamental questions:

a. What multi-sector planning and guidance can provide the requisite level of collaboration, both in advance and in real time, to sustain (or rapidly restore) the very most essential infrastructure systems and services?
b. How can such collaboration be structured in a way that is both consistent with federalism and the U.S. Constitution, and reflect the primary responsibility of infrastructure owners and operators for the resilience of their systems?

c. How should the United States and partner nations develop and deploy communication and coordination systems to support multi-sector operations that are widely-distributed, interoperable, and can operate in Black Sky events?

**EPRO Handbook III** addresses these questions and proposes options to strengthen multi-sector resilience.

Chapter I of the Handbook examines the explosive growth in infrastructure interdependencies, and how natural and manmade Black Sky hazards could produce crippling failures across and between infrastructure sectors. Based on those vulnerabilities, the chapter proposes criteria to prioritize cross-sector support operations in Black Sky events. The chapter then recommends measures to help such operations go forward through collaboration: 1) between infrastructure owners and operators; 2) between government actors operating in sector or agency silos; and 3) between sector leaders and their government and NGO counterparts.

Chapter II analyzes the requirements that multi-sector operations will entail for communication systems, and for the situational awareness and decision support capabilities they will need to host for industry, government and NGO leaders. Chapter II also describes how the BSX system is evolving to meet these needs, and identifies next steps for the buildout of the system.
CROSS-SECTOR COORDINATION CHALLENGES, AND STRATEGIES AND STRUCTURES FOR COLLABORATION

1. Economic Challenge: Powerful economic forces are driving the rise of cross-sector interdependencies, creating new sources of fragility for which the United States is utterly unprepared.

Compelling economic incentives are accelerating just-in-time inventory management, consolidation and reduction of excess capacity in distribution systems, and concentration of critical facilities. Halting these shifts would harm U.S. competitiveness and be wholly impractical. It is nonetheless essential to identify and mitigate the new vulnerabilities that these trends are creating for Black Sky response operations, including the delivery of food, fuel, chemicals for water treatment, and other vital supplies.
Recommendation: Transform cross-sector resilience into a prime focus for private sector, government, and NGO planning

The electrification of everything, the rise of the Internet of Things, and the rise of system autonomy are outstripping current efforts to understand and mitigate cross-sector vulnerabilities in “smart cities” and beyond. To improve our understanding, infrastructure owners and operators, their critical supply chains, and their government and NGO partners will need access to a comprehensive, multi-sector mapping and modeling capability. A modeling framework that could provide such capabilities would also need to leverage situational awareness and decision support tools to enable dynamic, real time response operations in complex catastrophes.

The Global Infrastructure Network Optimization Model (GINOM™) project will be essential for assessing these novel and potentially catastrophic sources of fragility, and will provide tools to support response, sustainment, and recovery operations. Other public and private sector modeling initiatives, especially those led by DHS and prominent industry organizations, will be essential to supplement the GINOM system.

2. Prioritizing Restoration Investments and Plans for Black Sky Scenarios: The United States lacks the criteria and information sharing systems necessary for prioritizing cross-sector sustainment and restoration operations

Individual sectors and utilities within them typically have their own priorities for sustainment and restoration, optimized for their specific industry and service areas. However, given the extensive infrastructure damage that multi-region Black Sky events will create, the United States needs a nationwide basis to determine which infrastructure services and functions across all sectors are absolutely most vital for: 1) preserving national security; 2) limiting long-term damage to the economy; and 3) preventing infrastructure breakdowns from creating humanitarian catastrophes.

In some cases, such prioritization will only be possible if it is based on planning and associated investment implemented well in advance of a catastrophe. Black start restoration of the grid, for example, will require advance planning to prioritize and invest in Black Sky hazard-protected, fuel-secure, regionally distributed segments of the nation’s cranking paths. Without such
advance planning and investment, power companies would be utterly dependent on whichever existing black start cranking paths and associated loads happen to survive the Black Sky hazard, and would be unable to significantly “prioritize” restoration operations in real time as a result. Similar prioritization efforts will not only be necessary in all sectors, but between them as well.

DHS has developed a methodological starting point to establish priorities on a multi-sector basis. In particular, as required by Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, DHS has created a “Section 9” list of especially critical infrastructure. But this cyber-focused list was never intended to be used as an all-hazards prioritization scheme to guide cross-sector sustainment and restoration in Black Sky outages, nor does it provide the granularity needed do so. Moreover, while DHS informs infrastructure owners whether they are on the list, the Department rarely tells them which – if any – Section 9 assets from other sectors operate in their service territory. The Section 9 methodology can nonetheless provide a valuable starting point for designing a similarly cross-sector focused effort.

**Recommendation: Build a Black Sky Prioritization List (BSPL)**

DHS and its industry and government partners should leverage the Section 9 methodology and many other (usually stove-piped) prioritization initiatives to build a consolidated, “user friendly” list of the most important services and facilities to sustain or restore in Black Sky events. Existing information sharing mechanisms should also be leveraged to ensure that cleared industry personnel are aware of the BSPL assets in their service territories and can plan for cross-sector sustainment and restoration operations accordingly.

3. **Private Sector Coordination**: The private sector is not adequately organized for cross-sector sustainment and restoration operations

Infrastructure owners and operators will need to play a leading role in defending and restoring their own systems in Black Sky events, and in prioritizing and providing cross-sector assistance. Industry leaders have

---

recently taken major steps forward to facilitate such collaborative decision-making. Most important, the coordinating councils of the electricity subsector, the financial services sector, and the communications sector have established a Strategic Infrastructure Coordinating Council (SICC) to develop and exercise cross-sector response plans and interface with government leaders.\(^8\)

However, building preparedness for Black Sky events will require the inclusion of a broader range of infrastructure sectors than included in the SICC. Such catastrophic events will also require industry leaders to coordinate sustainment and restoration operations in the face of unprecedented cross-sector failures, including major communications outages.

**Recommendation: Build on the SICC to create an expanded, operationally-focused organization for industry collaboration**

Infrastructure leaders should leverage the SICC and other emerging coordination mechanisms to create a **Cross-Sector Coordinating Council (CSCC)**, which will support broader cross-sector operational planning and coordinate incident response activities. The CSCC will need to account for the widely differing ways in which sectors are organized, and variations in the degree to which they are currently capable of coordinating support operations by their members. Such collaborative decision-making will nevertheless be essential in Black Sky events.

---


The U.S. national incident response system is focused on delivering Federal assistance to states and localities when their own resources prove inadequate. However, in Black Sky events, industry must lead efforts to sustain and rapidly restore critical infrastructure services to save lives and protect U.S. security. The current system, however, is poorly structured to facilitate industry-led operations.

Filling these gaps by building a new, separate response system only for Black Sky events would be unwise and politically impractical. The National Response Framework and the coordination mechanisms that it supports are so deeply embedded in the United States, and so closely aligned with the Federal system of government and key acts of Congress, that developing and maintaining a “just break glass” system solely for Black Sky events would be extraordinarily difficult.

Recommendations: Put government and NGO support for industry-led, cross-sector infrastructure operations at the heart of emergency management

The 2017 Power Outage Incident Annex provides a critically-needed basis for regional planning against the cascading failures that Black Sky hazards will create. However, in addition to fully engaging infrastructure owners and operators in such planning, emergency managers will also need to advance a score of other initiatives. Among the most important proposed in this volume:

- Federal Government Black Sky Support for States and Industry: Reinforce the ability of the Federal Government’s National Response Coordination Center (NRCC) to prioritize and help guide government support to industry.

Infrastructure owners and operators should pre-arrange with FEMA to include industry representation for all critical sectors in the NRCC.
and ensure that industry decisions made in the proposed CSCC are fully integrated into government response operations.

An especially important aspect of this approach will be a new effort to address two areas of Black Sky support.

a. **Expanded, Black Sky-Compatible Emergency Power Assets:**
   Crucial for enabling industry-led infrastructure sustainment and restoration operations on a multi-region basis will be ensuring adequate emergency power for the most critical facilities. Current emergency power capabilities are designed to address relatively local hazards. FEMA and the United States Army Corps of Engineers (USACE) should therefore acquire adequate, nationally deployed, Black Sky-protected emergency generators (and related equipment and technical support) to address anticipated emergency power needs in Black Sky events on a prioritized basis.

b. **Black Sky Certified Emergency Fuel and Other Supply Chain Resources:**
   Given the urgency of maintaining adequate supply chains for resources and services essential to infrastructure sustainment and restoration, FEMA and USACE should work with the CSCC to pre-designate categories of supply chain corporations as “Black Sky-certified” organizations. As one example, Black Sky-certified emergency diesel fuel delivery corporations will be essential to ensuring key critical infrastructure facilities will have a continued source of fuel for emergency power generation in such disasters. Government and industry stakeholders will need to ensure these (and other similar) capabilities, along with their critical supply chains, cover all U.S. regions. Close coordination with SLTT governments will also be essential as this initiative goes forward.

- **State Government Black Sky Support for Private Industry:**
  Leverage the unique responsibilities of Governors for disaster response
  Under the U.S. Constitution, governors are responsible for the health and safety of their constituents. At the state level, and with full
engagement of local, tribal and territorial governments, infrastructure owners and operators should partner with emergency managers to ensure that:

1. State priorities are taken into account in sustainment and restoration operations.
2. Government support for those operations is included in response planning and exercises.

- **Create a new Emergency Support Function (ESF): ESF-14, Cross-Sector Infrastructure Coordination**

The ESF system is a key coordination structure used by the Federal government for building, sustaining, and delivering response capabilities, including those necessary for sustaining and restoring critical infrastructure. However, ESFs are focused primarily on the delivery of government response capabilities and are poorly structured to help coordinate industry-government collaboration. By design, ESFs focus on specific response tasks and (in many cases) particular infrastructure sectors.

Government agencies, NGOs, and industry representatives should therefore collaborate to establish a new ESF focused on supporting and addressing the specific challenges posed by cross-sector sustainment and restoration operations in the catastrophes to come.
Restructuring the United States’ emergency response system to facilitate cross-sector support operations will be useless without survivable, widely-distributed, and interoperable systems for communication, coordination, and decision support.

Many infrastructure owners and operators have emergency communications systems that can help sustain their own functions in a blackout. FEMA, the FBI, state National Guard units, and a handful of other government organizations also have specialized, closely-held systems for dedicated use in manmade or natural disasters.

However, for multi-sector collaboration (as well as intra-sector operations), the United States will require communication and coordination systems that are widely deployed across all infrastructure sectors and their critical supply chains, and connected to (and interoperable with) a broad range of private and public sector partners. Those systems will also need the ability to:
• Survive EMP attacks, cyberattacks, catastrophic earthquakes, and other Black Sky hazards.
• Continue functioning in the absence of grid-provided power for a month or more.
• Withstand adversary efforts to disrupt communications or corrupt the integrity of data flows.
• Provide adequate means for critical voice and data connectivity necessary for sustainment and restoration operations across multiple regions of the United States.
• Gather and convey multi-sector situational awareness information essential to decision makers in all sectors, who will find themselves operating without any of their normal information resources.
• Provide a decision support engine, configured for local users’ unique, sector-specific requirements, that is adequate to help manage complex Black Sky catastrophes.

A widely, multi-sector deployed, interoperable, and Black Sky-survivable emergency communication and coordination system is a fundamental prerequisite to any infrastructure restoration and population sustainment operations in national scale catastrophes.

One example of such a system already exists. Since 1998, the U.S. Army has been relying on a survivable, widely-distributed command, control, and coordination system – the Blue-Force Tracker – in combat environments. Based on that proven technology and engineering approach, EIS Council and its partners are developing a Black Sky Emergency Communications and Coordination System (BSX™) to meet the specialized needs of infrastructure sustainment and restoration operations in catastrophic events.

---

Chapter II of this volume analyzes gaps in current U.S. capabilities for cross-sector communications and coordination. The chapter also examines how the BSX system is evolving to fill these gaps, describes the prototype system that is being developed, and identifies next steps for the buildout of the system.

Key findings and recommendations

1. **Current emergency communications systems cannot provide the multi-sector connectivity and interoperability that will be essential in Black Sky events.**

   Electric companies, water utilities, and other infrastructure owners and operators are making significant progress in acquiring fallback systems that can support their operations in blackouts. However, given the growing interdependencies between these sectors, and the need for close collaboration with NGOs and emergency managers, broad cross-sector connectivity will be vital for Black Sky response operations. No existing system, nor the current collection of disparate systems, can meet that need in a severely disrupted environment.

   **BSX design:** BSX is being engineered to provide a common communications system (including hardware and software) to support essential voice and data links between all critical infrastructure owners and operators, and their key government and NGO partners. BSX communications nodes will also be interoperable with any other emergency communications systems that survive the onset of a Black Sky event. In particular, BSX’s software will enable it to serve as a “bridge” between previously-incompatible communications systems, thereby expanding the BSX system’s reach and capacity.

2. **Long duration power outages will cause failures in many existing communications systems.**

   Most primary and backup communications systems are supported by emergency power generators. They also have at least limited on-site fuel supplies.
for those generators, and contracts for fuel resupply. However, blackouts lasting a month or more will put incredible stress on those emergency power capabilities, especially as fuel distribution and supply chains break down.

**BSX design:** Each deployed BSX communications node will have sufficient sources of power (including solar and/or wind, where applicable) to sustain operations for a minimum of 30 days. Depending on the node’s siting and specific operational requirements, this can be achieved in a number of ways. At critical sites, including those essential to infrastructure sustainment and restoration, BSX can rely on the facility’s own emergency power sources – without which the facility cannot operate, and communications capability will be of limited value. For more remote sites, BSX nodes can rely on power modules tailored to their operational needs. In all cases, BSX planning and deployment will include power requirement projections to facilitate power budgeting and ensure that the system maximizes its power efficiency. The deployed system will also include active network power management.

3. **Cross-sector operations will require communications links for vast numbers of users on a common system.**

Black Sky operations will require not only multi-sector and industry-government connectivity, but also very large numbers of deployed communications nodes. EIS Council analysis suggests that at least 200,000 interconnected nodes will be required across the United States.

**BSX design:** To meet such large-scale requirements for system distribution, the BSX system is placing a premium on affordability. The system is also being engineered to be “user-friendly.” Rather than requiring emergency personnel to have specific expertise, a packet router equipped with mission-specific software agents at
each site determines which radio, frequency, and communications links to use for all transmissions. This automation significantly decreases the technical complexity of operating the system.

4. Relatively few emergency communications systems are hardened to withstand EMP and other Black Sky hazards.

Ensuring that these systems will still be functional after years of infrequent use, and limited maintenance, will also be essential.

**BSX design:** BSX is being specifically designed and engineered to survive Black Sky hazards. The system and its components will be able to withstand an EMP attack and advanced cyber threats, as well as other natural and manmade hazards. BSX is also being engineered to be able to lie dormant at unmanned locations for years at a time, requiring only periodic testing, and is capable of quickly transitioning to operational mode when catastrophes strike.

5. Beyond communications and coordination, emergency systems should also provide other essential features to support Black Sky operations.

In addition to the need for interoperable, multi-sector communications capabilities on a nationwide scale, two additional challenges will be especially pressing in Black Sky events.

Decision makers in all sectors will need dependable situational awareness data to guide effective operational decision-making in complex catastrophes.

Given the remarkable challenges associated with infrastructure restoration and population sustainment on the scale envisioned for such catastrophes, an artificial intelligence-enabled decision support model will be a critical need.

BSX is being designed to host the situational awareness and decision support systems necessary for addressing these challenges, which are summarized below.
THE WAY FORWARD: BUILDING A SUITE OF BLACK SKY RESPONSE TOOLS AND TECHNOLOGIES

Societal breakdown will loom in Black Sky events unless the technologies we use to solve complex problems progress in line with the technological advancements that contribute to these challenges. As the organic hyper-connectivity and complexity of our infrastructure networks continue to spiral upward, we must develop the capability to map and model the dynamic operation and behavior of these networks. Infrastructure owners and operators must be able to understand critical interdependencies well enough to protect the system of systems, to make

Given the scale of a Black Sky catastrophe, technology to map complex interdependencies and automate sustainment and restoration decision support will be essential to prevent societal collapse.
the multitude of real time decisions needed to sustain society during large-scale infrastructure sustainment and restoration operations, and to minimize recovery times following a Black Sky event.

The emergency communications system described in the previous section can contribute to achieving these capabilities. Indeed, it is part of the EIS Council’s growing suite of tools being designed and developed for catastrophic event response. The BSX™ Resource Family includes the BSX system itself, the Situational Awareness Network Diagnostic (SAND™) System, and the Global Infrastructure Network Optimization Model (GINOM™).

Together, BSX and the key capabilities it hosts will perform three critical functions in Black Sky events.

**Essential BSX System Functions**

- **Providing Nationally Deployed, All-Sector Emergency Communication:** The system will provide voice and data communication to enable infrastructure support, population sustainment, response operations, and other Black Sky activities.

- **Hosting a Situational Awareness Hub:** BSX will host operation of the Situational Awareness Network Diagnostic (SAND™) System, now in initial development. SAND is being designed to remotely acquire diagnostic data from both available and newly deployed sensors embedded in critical infrastructure, resource, and service sectors and their supply chains. This critical capability provides a unique multi-sector, real time view that will be essential for decision makers in catastrophic events.

- **Hosting a Multi-Sector Model and Simulation:** BSX is also designed to host operation of the Global Infrastructure Network Optimization Model (GINOM™). GINOM is a software-driven, multi-infrastructure modeling and simulation framework. Such a system will be essential to assist decision makers in all sectors as they work to “manually” support the wide array of (normally self-sustaining) resource flows necessary to enable infrastructure restoration and sustain the affected
population. Given the complexity of this task, interdependency mapping and artificial intelligence (AI) support from GINOM will be essential to help these managers optimize prioritized, time sensitive decisions in responding to the vast array of unpredictable events and the many dimensions of intricate challenges that will emerge in complex catastrophes.

This set of complementary tools and systems will operate together to help the nation respond to Black Sky disasters. BSX, now in the early stages of prototype development, will support voice and data communication, acquire diagnostic data from SAND and other sources, and provide an expandable server network to host GINOM in severely disrupted scenarios. GINOM will provide government and industry leaders with a decision-support capability, giving them the information they need to understand, prioritize, and meet the vital support requirements of lifeline infrastructures.

GINOM will help the infrastructure owners and operators at the heart of restoration operations and their government partners implement the objectives outlined in Chapter II. While prioritization initiatives like the proposed BSPL will be crucial to emergency preparedness, these priorities will need to be fluid, adapting in real time to outages and successful restoration operations. Attempting to manually aggregate and analyze the amount of data required to do so would be impossible.

GINOM will also provide valuable capabilities before Black Sky hazards strike. Its comprehensive modeling tool will be vital to understanding the complex interdependencies of our critical infrastructure systems, allowing industry to optimize infrastructure efficiency and identify resilience gaps. Over time, a comprehensive model of global infrastructure networks can also be used to recommend policies and investments that could shift infrastructure interconnectivity to reduce vulnerable interdependencies.

These tools will be most effective in Black Sky events if their intended users are able to test and train on their functions in exercises. EIS Council successfully completed the first annual EARTH EX* exercise in August 2017, providing participants with a multi-sector, international exercise to evaluate and improve
restoration support, preparedness, response, and recovery plans for severe hazards. EARTH EX is designed to improve resilience to Black Sky outages by allowing participants the opportunity to evaluate tools and strategies for catastrophic event response. As the BSX Resource Family continues to develop and improve, future EARTH EX exercises will provide developers and intended users a chance to become familiar with, test, and optimize their utility in Black Sky events.
CHAPTER ONE

SUSTAINING AND RESTORING CRITICAL INFRASTRUCTURE IN BLACK SKY EVENTS

Cross-Sector Strategies and Coordinating Mechanisms
INTRODUCTION

When extreme catastrophes strike, disruptions of the electric grid and other infrastructure will create immense challenges for saving lives, preserving national security and ensuring societal continuity. Meeting these challenges will require new investment strategies and coordinating mechanisms to help multiple, interdependent infrastructure sectors help each other sustain and restore vital services.

Many infrastructure owners and operators are improving the resilience of their own systems against catastrophic hazards. However, massive earthquakes, electromagnetic pulse attacks, and other severe hazards still threaten to simultaneously cripple a broad range of infrastructure systems. This is particularly problematic in today’s hyperconnected world, where

Massive earthquakes, electromagnetic pulse attacks, and other Black Sky hazards will simultaneously cripple all infrastructure systems and sectors.
infrastructure sectors depend on each other to function. The Department of Homeland Security’s (DHS) Power Outage Incident Annex provides a valuable framework to address many of these interdependencies. However, unless sector leaders and their partners also create detailed plans to strengthen their shared resilience and build survivable communications and coordination mechanisms to enable cross-sector response operations, failures will cascade across all of the systems on which the United States depends.

This chapter examines how the United States and partner nations can transform their infrastructure interdependencies into bulwarks of resilience. The chapter analyzes how infrastructure owners and operators, key resource providers, and non-governmental organizations (NGOs) responsible for mass care can partner with government officials to sustain and restore essential services when catastrophes strike. In particular, the chapter focuses on building cross-sector preparedness for Black Sky events – i.e., catastrophes that disrupt electric service to major portions of the United States for a month or more, and damage or destroy other infrastructure essential for societal continuity.
1. Cross-Sector Resilience: Challenges and Imperatives for Progress (Section II)

The growing interdependence of U.S. infrastructure sectors will make cross-sector resilience increasingly necessary, yet also more difficult to achieve.

The deepening mutual dependency between the natural gas and electric subsectors provides a case in point. Modern gas turbine power generators provide an increasingly cost-effective means of generating electricity and are becoming the predominant source of power in many U.S. regions. At the same time, natural gas systems increasingly rely on electricity for pipeline compressors that keep gas flowing to power generators.

Rising interdependencies between critical infrastructure sectors will make cross-sector resilience both essential, and more difficult to achieve.
These gas-electric interdependencies create efficiencies, but also shared vulnerabilities. When Black Sky events create extended, multi-state blackouts, the loss of power will disrupt electric-powered compressors and other gas system components. In turn, disrupted gas systems will be unable to provide fuel to power generators, including those essential for re-energizing the electric grid and restoring power to gas systems.

To guard against these mutually-reinforcing failures, some natural gas systems have placed increasingly robust backup power systems at compression stations and other electricity-dependent facilities. Many thousands of hospitals, food distribution centers, communications facilities, water systems, and other providers of critical services have also installed backup power generators, as well as on-site storage for diesel and other liquid fuels to power them.

However, in long duration blackouts that cover major portions of the United States, continued operation of these facilities will nonetheless create immense cross-sector requirements for emergency generators and fuel resupply. These power outages, as well as the direct impact of earthquakes and other Black Sky events would also severely damage the communications and transportation infrastructure on which such resupply operations would depend.

Emergency generator supplies and the liquid fuel refining and distribution systems in the United States are inadequately prepared to meet these challenges. Driven by economic imperatives to cut costs and maximize efficiencies, U.S. liquid fuel refining and distribution systems are becoming increasingly consolidated, streamlined, and free of the excess capacity that would be vital in a Black Sky event. Current reserves of emergency generators, both those in the nation’s emergency management system and those available from private sector suppliers, have generally been adequate – though often just barely – in outages
caused by natural hazards, such as Superstorm Sandy and more recent weather-induced disasters. However, for the much more severe power outages that Black Sky hazards would create, these inventories would be utterly inadequate to provide the emergency power needed by all 16 critical infrastructure sectors.

Similar challenges exist for the U.S. food system, the pharmaceuticals industry, and a wide range of other suppliers of critical goods and services. In all of these industries, powerful economic incentives are driving consolidation of “just-in-time” production and distribution systems, and the stripping out of excess infrastructure capacity that would be essential for cross-sector resilience in Black Sky events. These industries will also create additional demand for emergency generators and fuel that will be impossible to meet in long duration, wide area power outages.

The hurricanes and wildfires of 2017 have highlighted the severity of these challenges. Most notably, the damage that Hurricane Maria inflicted on Puerto Rico’s power grid and liquid fuel distribution systems caused cascading failures across all other sectors. In turn, those failures created immediate crises in sustaining the island’s population, while simultaneously creating insuperable obstacles to power restoration.¹

The 2017 hurricanes also exemplified how the streamlining and consolidation of the production and distribution of essential commodities create new challenges for disaster preparedness. Much of the United States relies on pharmaceuticals and medical supplies produced in Puerto Rico. When Maria struck, the disruption of those supplies posed a potential threat to healthcare facilities and services on a nationwide scale.²

---


Hurricane Maria also highlighted the way in which the geographic scope of an event will help drive the scale and complexity of cross-sector operations. The devastation wrought by Hurricane Maria represents a “bounded” Black Sky event. Power outages in Puerto Rico lasted months for many of the island’s citizens, and greatly magnified the threats to public health and safety that the hurricane inflicted. The distance of the island from the U.S. mainland created further challenges for conducting response operations. However, Maria left those mainland response capabilities unscathed. A catastrophic earthquake, nationwide cyberattack, or other Black Sky event, would cripple infrastructure across vast regions of the United States, creating immense and unparalleled challenges for sustainment and restoration operations. Helping infrastructure owners and their emergency response partners prepare to meet such challenges is the focus of this Chapter.

a. **Implications for Preparedness against Natural Hazards**

Accelerating structural changes in U.S. infrastructure will magnify the difficulty of saving and sustaining lives in Black Sky catastrophes produced by earthquakes and other especially destructive natural hazards. Recent exercises, including the 2016 Cascadia Rising exercise (based on the scenario of a 9.0 magnitude earthquake and subsequent tsunami striking the Pacific Northwest), have cast new light on the significance of infrastructure resilience for disaster response.

Washington State’s draft after-action report (AAR) from Cascadia Rising found that urban search and rescue and other immediate life-saving operations can reduce initial casualties in such events. However, the damage to electricity and other infrastructure will threaten lives on a vastly larger scale due to escalating food and water shortages, breakdown of waste removal and sanitation, and the loss of other critical services. The result: once the earthquake strikes, “the clock is ticking to a humanitarian disaster.”

---

Preventing such outcomes will require twin strategies for infrastructure resilience. First, by selectively hardening crucial infrastructure components, and prioritizing the sustainment of services to hospitals, food distribution centers, and other essential facilities, infrastructure owners and operators can help limit risks to public health and safety. Second, because earthquakes and other severe hazards will still cause extensive damage, infrastructure owners and operators will need the ability to prioritize the restoration of service in ways that help avert humanitarian disaster. Key prerequisites for success (all of which are examined later in this chapter) include:

- Support from public sector leaders, including emergency managers, elected officials, and regulators. Engagement with regulators will be especially important for enabling cost recovery for prudent investments in resilience.
- Sharing of information across interdependent infrastructure sectors so owners and operators can identify key opportunities for mutual support to sustain and restore service, and build Black Sky “Playbooks” for emergency operations.
- Improved plans to both enable and prioritize the multi-sector coordination that will be critical in such events. Particularly critical examples of this need include the delivery of emergency generators and fuel for critical facilities, enforceable standards and requirements for generation capacity and testing, and increased capacity to meet the enormous cross-sector demand for such support in Black Sky events.

b. Manmade Threats

Attacking hyperconnected infrastructure sectors could not only enable adversaries to jeopardize U.S. public health and safety, but also threaten the ability of key military bases and other national security facilities to carry out their missions. Building infrastructure resilience to meet these security challenges will require measures over and above those required against natural hazards. Yet, doing so will also yield especially significant benefits, including that of helping to deter attacks on critical infrastructure.

The U.S. Department of Defense (DOD) increasingly relies on domestic installations to conduct and support military operations abroad. The Department’s Mission Assurance Strategy (2012) noted that because
military bases depend on the power grid and other civilian infrastructure sectors, adversaries could strike that infrastructure to disrupt base operations, thereby crippling the ability of Defense installations to execute their Mission Essential Functions (MEFs).\(^4\)

Military bases and other facilities vital for national security have responded to this risk by strengthening their ability to serve mission-critical loads with backup power generators. A growing number are also partnering with electric utilities to develop microgrids that can operate as “power islands” if adversaries disrupt electric service to the installation.

However, because many of these microgrids rely on gas turbines to generate power, the flow of natural gas will be crucial for overall installation resilience (especially if adversaries attack gas and electric power systems at the same time). Major military bases and the communities where their employees live also depend on civilian owned and operated water systems, hospitals, food and pharmaceutical supplies, transportation networks, and other critical infrastructure. Building plans and capabilities to sustain essential services to Defense installations and associated communities, and to rapidly restore service when disruptions occur, will therefore be essential for U.S. security.

These security challenges are also becoming more difficult to overcome. A February 2017 report by the Defense Science Board found that given the United States’ extraordinary vulnerability to cyberattacks by Russia and China, Federal Departments should partner with infrastructure owners and operators to “harden the most vital U.S. critical infrastructure” against attack, especially for infrastructure that serves military functions.\(^5\) Doing

---


so will require not only sector-specific resilience initiatives, but also enhanced strategies and mechanisms to enable cross-sector planning and real-time coordination for infrastructure sustainment and restoration to support critical Defense functions.

The same requirements will exist to harden critical infrastructure against electromagnetic pulse (EMP) weapons and strikes that combine cyber and kinetic attacks. Electric utilities are making significant progress against both threats; accelerating their progress and sharing best practices with other vulnerable sectors will be vital as threats continue to intensify.

Adversaries could also seek to strike critical infrastructure and/or disrupt sustainment and restoration operations in innovative ways. Improvements in drone technology increase the potential for adversaries to use unmanned aerial vehicles (UAVs) to attack U.S. infrastructure, especially if they are equipped with Improvised Electromagnetic Interference Devices or other advanced payloads. In addition to launching kinetic attacks against electric substations or other key infrastructure nodes, adversaries could also deploy

---

active shooters to disrupt restoration operations. Adversaries may not even need this follow-on kinetic threat to achieve the same result. False but carefully-crafted social media reports that utility workers had been shot (or that toxic clouds were being released from chemical facilities) could also impede restoration efforts and create major challenges for industry-government communications with a concerned public.

**Cross Sector Resilience: Section Overview**

Section II highlights how the increasingly severe threat environment will create new challenges for cross-sector resilience. The section also analyzes emerging requirements for government to help industry leaders sustain and restore critical infrastructure service in severe outages, including:

- Enhanced strategies and mechanisms to expand traditional support activities, including ensuring the availability and delivery of critical tools, “consumables” (water treatment chemicals, emergency generator fuel, etc.) and other resources. Expanded government assistance efforts will also help provide security for critical infrastructure workers and affected populations, road clearance and debris removal to assist power restoration, and other scaled-up versions of familiar support missions.
- New support missions (e.g., countering information warfare campaigns that seek to incite panic and disrupt restoration operations).
- Innovative cost recovery mechanisms for targeted private sector investments in resilience, especially those necessary to help prevent catastrophic damage to societal continuity, national security, and the economy.

Repairing power lines and replacing damaged transformers (Source: FEMA)
2. **Black Sky Prioritization**: Strategies to Identify and Protect Critical Facilities, Supply Chains, and Assets (Section III)

Given the scale of devastation that Black Sky events will inflict, it will be impossible to sustain uninterrupted service to all customers for electricity, water, and other essential resources and services. Nor will it be possible to accelerate the restoration of services and access to key resources for all such customers. Indeed, there may even be a need to divert resources from (or shut down) functioning systems to sustain or restore more critical ones. To ensure national survival against Black Sky hazards, strategies to enhance sustainment and restoration efforts will need to provide for both prioritizing and strengthening the facilities, supply chains, and functions that are most important for saving lives, preserving national security, and preventing long-term, unrecoverable damage to the U.S. economy. Government authorities at the Federal, state and local level must also address the added challenges of coordinating the process for implementing such prioritization strategies with the private sector, communicating these priorities to the American public, and facing public criticism for doing so.

Most infrastructure sectors already have plans for prioritized sustainment and restoration of service. In many cases, such as the restoration of electricity to nuclear power plants, existing prioritization criteria used by infrastructure owners and operators will be essential for preparedness against Black Sky hazards. However, given the unprecedented duration of projected disruptions in these complex catastrophes, the United States and its security partners need new strategies and mechanisms to ensure optimal prioritization.

a. **“Baking-in” Service Sustainment and Restoration Priorities within Infrastructure Sectors**

Given the extensive damage that Black Sky hazards will inflict on infrastructure systems, it will be essential for the owners and operators of those systems to identify the most critical components within them, and to prioritize hardening investments and emergency planning to help
those components survive or be quickly brought back to service in a severe outage. These priorities must be “baked in” to system restoration plans, as real-time coordination and decision making – especially if it involves communication between multiple utilities and sectors – will be near-impossible at the onset of catastrophic outages.

Power companies have considerable expertise in assessing the criticality of their own system elements and using those assessments to strengthen preparedness against manmade and natural hazards. Consistent with the North American Electric Reliability Corporation (NERC) critical infrastructure protection standards, electric companies identify especially vital substations and other system components, and prioritize their plans for sustainment and restoration accordingly.7

A growing number of water utilities, natural gas transmission systems, key resource providers, and other companies are now advancing their own sector-specific prioritization initiatives. Section III provides an overview of how the EIS Council-hosted EPRO Black Sky Playbook development process is supporting these efforts to strengthen resilience within infrastructure sectors.

b. Cross-Sector Support for Prioritized Sustainment and Restoration

The Playbook initiative also helps infrastructure owners and their partners meet an additional requirement for Black Sky preparedness: building shared resilience between interdependent sectors. Unless utilities and other key service providers can prioritize their cross-sector support requirements and embed those priorities in effectively-exercised sustainment and restoration plans, Black Sky response operations are sure to fail.

In addition, to effectively employ such plans and adjust them to meet unforeseen problems, infrastructure owners will also require survivable, real-time connectivity with a broad range of private, public, and mass-

---

care NGO partners. In particular, they will need situational awareness, communication, and decision support tools to help them prioritize support operations to meet the most dire requirements for cross-sector sustainment and restoration.

This Handbook highlights a number of such tools that are already under development. Chapter II examines the Black Sky-compatible Emergency Communication and Coordination System (BSX\textsuperscript{TM}). That system is configured for resilience against all Black Sky hazards and will be able to operate independently of national telecommunications assets. BSX is also designed to be fully interoperable with any other emergency communication systems that survive a Black Sky event. In addition, BSX is configured to support broad, multi-sector distribution, utilizing communications nodes designed to be self-powered for 30 to 60 days of operation.

However, decision makers will need more than basic voice and data capabilities in Black Sky events. They will also need tools to provide for multi-sector situational awareness in severely disrupted environments, supported by modeling to help them plan and conduct prioritized cross-sector support operations. BSX is being designed to host two such tools that are already under development. The Situational Awareness Network Diagnostic (SAND\textsuperscript{TM}) system will provide BSX-based access to any available system status or diagnostic reporting assessments. The Global Infrastructure Network Optimization Model (GINOM\textsuperscript{TM})\textsuperscript{8} will span and integrate both SAND data and selected infrastructure models to provide real-time decision support for government, private sector, and NGO leaders.

c. **Identifying Critical Facilities, Supply Chains, and Supporting Assets**

Government agencies will need to play a key role in determining which assets merit prioritized sustainment and restoration of service.\textsuperscript{9}

\textsuperscript{8} The Global Infrastructure Network Optimization Model (GINOM) project is an EIS Council-led initiative currently under development. More information will be available as the project progresses.

\textsuperscript{9} The term critical assets as used in this chapter falls within the definition of critical infrastructure found in Executive Order (EO) 13636: “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would
Infrastructure owners and operators may not be aware of all of the vital facilities that fall within their service area, especially as market forces drive continued streamlining and supply chain concentration for life-sustaining resources.

The Department of Homeland Security (DHS) can help identify such facilities. DHS’ “Section 9” list provides a prime starting point to do so. That list includes a stringently-defined subset of infrastructure facilities that are essential for national security, the economy, and public health and safety. But the Section 9 list focuses only on cyber threats. This chapter examines how DHS and its partners can build a comprehensive Black Sky Prioritization List (BSPL) optimized for cross-sector resilience against all hazards.

Moreover, DHS does not tell gas companies, electric utilities, and other service providers which facilities beyond their own sectors are in their service areas. While infrastructure owners and operators have the most recent and accurate data on their own configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data with DHS. Section III of this chapter examines opportunities to strengthen such two-way information sharing to help guide the sustainment and restoration of critical services in catastrophic outages.


10 As required by Section 9 of EO 13636, the Secretary of Homeland Security maintains a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.” Using the Section 9 list as the basis for Black Sky planning would require the identification of key facilities in non-cyber incidents as well (though substantial overlap with the cyber-driven list would probably exist). Incidents caused by non-cyber hazards as well. See: Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
3. **Infrastructure Owners and Operators: Cross-Sector Planning and Coordination for Black Sky Resilience (Section IV)**

The owners and operators of critical infrastructure are uniquely well-positioned to identify the assistance they will need to sustain service in Black Sky events. Their knowledge and expertise will also be essential in planning for and prioritizing integrated, multi-sector sustainment and restoration operations in Black Sky scenarios. Moreover, they own the resources necessary to conduct these operations. Accordingly, sector leaders and their employees must be at the heart of initiatives to strengthen cross-sector resilience.

Important cross-sector planning is already underway. As noted above, companies in a growing range of sectors are developing Black Sky Playbooks to identify their sector-specific resilience needs and requirements for mutual support. They are also building company-specific plans to assist each other, especially between electric utilities and natural gas companies. These Playbooks should be extended to encompass the full range of sectors and partners necessary to protect national security and public safety in catastrophes. The Power Outage Incident Annex (POIA) also provides a framework to guide planning efforts by FEMA regions.

Of course, when Black Sky hazards strike, infrastructure operators will need to revise their Playbooks and other planning efforts to fit the specific exigencies of the event. Some sectors already have mechanisms to coordinate response efforts within their own sector, which may be viable for more limited disasters, that can serve as a starting point for this Black Sky coordination need. The electric subsector, for example, has organizations to coordinate mutual assistance operations and conduct other emergency functions (including
coordination with government through the Electricity Subsector Coordinating Council, or ESCC).

What is missing is an industry-led mechanism to both plan and coordinate cross-sector operations for extreme, complex catastrophes. Building on a proposal by the National Infrastructure Advisory Council, the electric, financial services, and communications sectors are exploring how decision makers from these sectors might develop coordinated action plans and agreements to implement them.\footnote{Testimony of Thomas I. Farmer, Chair, Cross-Sector Council Partnership for Critical Infrastructure Security, Before the U.S. Senate Committee on Homeland Security and Government Affairs, “Hearing on Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities and Solutions, May 18, 2016, http://www.hsgac.senate.gov/hearings/assessing-the-security-of-critical-infrastructure-threat-vulnerabilitiesand-solutions.}

The communications sector has developed additional coordination options, including the creation of an “enablers” group of Internet and Communications Technology (ICT) companies critical for supporting cross-sector responses to catastrophic events.\footnote{Homeland Security Advisory Council, Final Report of the Cybersecurity Subcommittee: Part I – Incident Response, June 2016, p. 14.}

Section IV of this chapter examines options to strengthen mechanisms for cross-sector collaboration, and to move beyond strategy and policy coordination to guide actual operations. In particular, the chapter proposes the creation of a Cross-Sector Coordination Council (CSCC) that would build on existing coordination mechanisms and provide the greatly expanded industry collaboration that Black Sky events will require.

4. Revamping the U.S. Incident Response System: Government Support for Cross-Sector Operations (Section V)

The current U.S. incident response system is focused on delivering Federal assistance to states and localities when their own resources prove inadequate. However, to save lives and protect U.S. security in Black Sky events, industry-led efforts to sustain and rapidly restore critical infrastructure services must be at the heart of response operations.

Significant improvements in response policies, doctrine, and organizational arrangements will be necessary to integrate such industry-led efforts into
publicly-led emergency management. Three opportunities for progress will be especially important.

- **Cross-Federal integration.** In the aftermath of Superstorm Sandy, a growing number of Sector-Specific Agencies (SSAs) have been improving their ability to coordinate incident response efforts within their respective infrastructure sectors. However, for cross-sector operations, much stronger unity of effort will be needed across the Federal government to help prioritize and support industry-led efforts, and provide a counterpart to the proposed Cross-Sector Coordinating Council (CSCC). Section V of this chapter examines options to meet these requirements, including strengthening industry participation in the National Response Coordination Center (NRCC).

- **Federal-State coordination.** Governors are responsible for public health and safety in their states, and will play a particularly central and key role in helping industry prioritize response operations. However, Black Sky events will damage and destroy infrastructure across major portions of the United States and therefore create immense challenges for prioritizing sustainment and restoration operations between states. Section V recommends how government leaders can help insulate infrastructure owners and operators from the intense political pressure such events will create, and strengthen unity of messaging as competing priorities come to the fore.

- **Revamping the Emergency Support Function (ESF) system for cross-sector infrastructure operations.** ESFs provide the primary state and Federal coordinating structures for building, sustaining, and delivering response capabilities. However, the ESF system is focused on delivering government capabilities; many ESFs provide for only limited industry

---

participation. Moreover, ESFs are heavily stovepiped. Section V proposes options to remedy these shortfalls, including the creation of a new ESF dedicated to planning, developing, and implementing the operations that will be most needed in Black Sky events: Cross-Sector Coordination (ESF-14).
Following hurricane Maria, Puerto Rico’s island-wide, long duration power outage became one of the most recent, tragic examples of a (bounded) Black Sky event, with cascading failures of nearly all the island’s interdependent infrastructures.

II | CROSS-SECTOR RESILIENCE: CHALLENGES AND IMPERATIVES FOR PROGRESS

A growing number of sectors are not only improving their own resilience against natural and manmade hazards, but also working with other sectors to understand their interdependencies and improve their mutual resilience. Collaboration between the electric and natural gas subsectors is rapidly improving and needs to be sustained. Multi-sector exercises and emergency planning initiatives involving water systems, communications companies, the financial services sector, and other industries are expanding as well.

Rising infrastructure fragilities, sector interdependencies, and threats are increasing the risk of cascading, catastrophic infrastructure failures.
Despite these efforts, three trends are increasing the risk that catastrophic failures will cascade across U.S. critical infrastructure.\(^\text{14}\)

- **Emerging Infrastructure Fragilities**
  In the continuing drive for efficiency, many infrastructure sectors are expanding their automation, and making a range of other changes that are creating new sources of potential fragility.

- **Complex Cross-Sector Interdependencies: The Emerging System of Systems**
  The same drive for improving efficiency and service is encouraging steady growth in cross-sector integration, creating more pervasive and complex interdependencies.

- **Threats to Cross-Sector Resilience: The Strategic Challenge**
  Adversaries are aware of these growing interdependencies. We should expect them to target critical nodes and single points of failure accordingly to exacerbate cascading failures across multiple sectors. Even absent this nefarious intent, severe natural hazards will also induce cross-sector, mutually-reinforcing outages. Building strategies that account for and mitigate these threats is essential for national security and societal continuity.

---

\(^{14}\) Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, defines critical infrastructure as the “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” PPD-21 also identifies the 16 infrastructure sectors that fall within this definition, and lists the Sector Specific Agencies (SSAs) responsible for coordinating Federal support for the resilience for each sector. White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience, February 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
A. Emerging Infrastructure Fragilities

The American Society of Civil Engineers (ASCE) provides an especially useful snapshot of the current resilience of U.S. infrastructure as a whole. Every four years, the ASCE releases a report card for infrastructure sectors based on factors including condition, funding, maintenance, public safety, and resilience.\textsuperscript{15} The 2017 Infrastructure Report Card finds that despite ongoing measures to improve resilience, the cumulative grade for U.S. infrastructure as a whole is a D+, the same abysmal grade as four years ago.\textsuperscript{16}

Many industries that will be essential for saving and sustaining lives in Black Sky events helped pull down this overall grade. The water sector, for example, received a D. The key reasons:

\textit{Many of th[e] pipes [in U. S. water systems] were laid in the early to mid-20th century with a lifespan of 75 to 100 years. The quality of drinking water in the United States remains high, but legacy and emerging contaminants continue to require close attention. While water consumption is down, there are still an estimated 240,000 water main breaks per year in the United States, wasting over two trillion gallons of treated drinking water. According to the American Water Works Association, an estimated $1 trillion is necessary to maintain and expand service to meet demands over the next 25 years.}\textsuperscript{17}

Other Black Sky-essential sectors received similar grades. In each case, aging components and limited capacity represent serious problems for infrastructure resilience. In addition, these shortfalls are creating such fundamental needs for investment that even modest costs associated with Black Sky resilience

\textsuperscript{15} The American Society of Civil Engineers assesses infrastructure resilience in terms of the following criteria: “What is the infrastructure system's capability to prevent or protect against significant multi-hazard threats and incidents? How able is it to quickly recover and reconstitute critical services with minimum consequences for public safety and health, the economy, and national security?” “What Makes a Grade?,” American Society of Civil Engineers, 2017, http://www.infrastructurereportcard.org/making-the-grade/what-makes-a-grade/.

\textsuperscript{16} “America’s Grades,” American Society of Civil Engineers, 2017, http://www.infrastructurereportcard.org/americas-grades/. Infrastructure in the D category is “in poor to fair condition and mostly below standard, with many elements approaching the end of their service life.”

\textsuperscript{17} “Drinking Water,” American Society of Civil Engineers, 2017, http://www.infrastructurereportcard.org/cat-item/drinking-water/.
mandates that are key to societal continuity in a complex catastrophe are becoming more difficult to address.

The U.S. road transportation systems exemplify these problems. Black Sky events will put a premium on the survivability of tunnels, bridges and other potential transportation choke points. Adequate road capacity to support surge operations will also be essential. At present, however, more than two out of every five miles of America's urban interstates are congested, and an $836 billion backlog exists of unmet highway and bridge capital needs. The bulk of the backlog ($420 billion) is in repairing existing highways, while $123 billion is needed for bridge repair and $167 billion for system expansion.18

As infrastructure investment goes forward, including those proposed under the Trump Administration’s infrastructure initiatives,19 building resilience features into those projects from the start will be essential for Black Sky preparedness. Previous EPRO® Handbooks have identified options to help do so for a range of infrastructure sectors. However, planners will need to account for fundamental changes in the architecture of U.S. infrastructure, both within specific sectors and in the emerging “system of systems” on which multi-sector response operations will depend. Legislators and regulators should also give special consideration to the need for specific funding streams dedicated to strengthening infrastructure resilience.

1. The Drive for Efficiency: Consequences for Resilience

The economic imperatives to maximize system efficiencies are creating new problems for ensuring the availability of food, pharmaceuticals, liquid fuels, and other supplies that will be essential to save and sustain lives in Black Sky events.

---


One such problem stems from the centralization of distribution operations into a small number of extraordinarily large facilities, often located further from the populations they serve. In their drive to take advantage of economies of scale and reduce operational costs, distributors of essential commodities are increasingly concentrating their operations in a dwindling number of locations. This “over-concentration reduces the flexibility of the supply chain to react to changes in the environment and leads to a fragile supply chain that is increasingly susceptible to disruptions.”

This emerging reality creates new imperatives for Black Sky resilience planning.

Food supplies provide a case in point. In many U.S. cities, a handful of distribution centers meet the feeding needs of millions of citizens. In New York City, for example, about 60 percent of the city’s produce and approximately half of the city’s meat and fish pass through Hunts Point Food Distribution Center (FDC). The centralization of these distribution assets creates single points of failure that can have massive consequences if disrupted. Moreover, in the drive to maximize effectiveness, this centralization process has gone forward without adequately accounting for obvious risk factors. Close to 28 percent of the Hunts Point FDC site is at risk of flooding.

Distribution system centralization is accelerating for other critical disaster response supplies as well, encouraged by another major trend creating resilience challenges: mergers and acquisitions. As this trend continues in pharmacies and provider markets, for example, wholesalers and distribution system owners are under increasing pressure to reduce their own costs by consolidating and achieving economies of scale in storage and distribution.

---


22 Ibid.
facilities. Consolidation in liquid fuel refineries is going forward at a “frenzied” pace. Liquid fuel distribution systems, including pipelines and truck delivery companies to serve end users, have also become increasingly consolidated and restructured to eliminate excess capacity.

The rise of just-in-time inventory management poses a similar risk, creating new challenges for ensuring adequate resources will be available in Black Sky scenarios to sustain affected populations and support infrastructure restoration operations. As Toyota Motor Company initially demonstrated, a wide range of sectors can save money by ordering and receiving inventory only as it is needed. Companies using just-in-time strategies do not hold “safety stock” and operate with low inventory levels. However, when catastrophes strike, providers of medical supplies, chemicals for water treatment, and other resources that have inventory sufficient only for just-in-time needs will be extraordinarily vulnerable to transportation and supply chain breakdowns. Developing Black

---


Sky resilience approaches that account for all of these trends represents a key requirement to ensure national security and societal continuity in complex catastrophes.

The disruption of liquid fuel distribution during Superstorm Sandy highlights the combined risks created by these three trends. Gas stations in New York City, for example, generally have much less than four days’ worth of fuel supply on hand. Moreover, many pumping stations along liquid fuel pipelines that service the region were not hardened against extreme weather. Together with the lack of redundancy in liquid fuels infrastructure and insufficient market flexibility to respond to disruption, Sandy produced fuel shortages for public safety vehicles (and private cars) that required a massive DOD resupply effort to remedy.

The risks created by these trends are magnified by an additional factor: the concentration of critical facilities and functions on a larger, multi-region scale. Chicago has become the central distribution hub for much of North America. With the third largest intermodal port in the world, and three major airports, the Chicago urban area moves around $3 trillion worth of goods annually, including food and other essential commodities.


29 Ibid., at p. 142.
Increased distribution distances also pose greater risks of disruption and increase the area over which repair and restoration must take place before goods can flow again. New York, Chicago, Los Angeles, Atlanta, and Dallas operate as trading depots for the entire country, consolidating the movement of goods in every direction and within their surrounding regions. These centralized functions and facilities place immense pressure on supporting infrastructure by increasing the ‘distribution distance’ that goods need to travel in case of a disaster – from neighborhood or region to inter-region. Disruption of that infrastructure by natural hazards or manmade threats would create multi-region effects; we should assume that adversaries will target their attacks accordingly.

Repairing natural gas infrastructure after Hurricane Sandy (Source: FEMA)

Finding

Rather than seek to reverse the trends that are re-architecting U.S. infrastructure, infrastructure owners and operators and emergency response personnel should account for their effects by 1) protecting especially critical system components, and 2) adapting response and sustainment operations to account for trends in infrastructure modernization.

Compelling economic incentives are accelerating just-in-time inventory management, industry consolidation, reduction of excess capacity in distribution

systems, and concentration of critical facilities. Halting these shifts would harm U.S. competitiveness and be wholly impractical. It is nonetheless essential to identify and mitigate the new vulnerabilities that these trends are creating for Black Sky response operations, including the delivery of food, fuel, chemicals for water treatment, and other vital supplies.

**Recommendation (a): Private sector leaders, in coordination with their government and NGO partners, should build Black Sky Playbooks to reflect emerging resilience challenges.**

Progress towards this goal is already underway. A growing number of infrastructure owners and operators are developing Black Sky Playbooks through the EPRO SECTOR planning framework and other initiatives which not only specify resilience missions, required capabilities, and concepts of operation within their own sectors, but (using a systems engineering approach) are systematically mapping their dependencies on other sectors and developing plans for cross-sector support. These EPRO Black Sky Playbooks and other, similar planning initiatives will need to be constantly refined to account for efficiency-driven shifts in infrastructure architecture and the new vulnerabilities they are creating.

**Recommendation (b): Industry and government should partner to increase inventories of selected, Black Sky-critical assets and resources, and strengthen the resilience of their supply chains and distribution systems.**

Accounting for just-in-time inventory management and distribution system fragility will be essential to developing and executing Playbooks. Emergency power assets offer a prime example. Black Sky outages will create an enormous mismatch between requirements for deployable backup generators and diesel fuel, and the ability of industry and government to meet that demand in a severely disrupted environment. Government and industry leaders should partner to expand and protect inventories of such Black Sky-essential assets, and ensure plans and capabilities exist to effectively distribute them to water systems, regional hospitals, and other key facilities.

---

Specifically, expanding existing stakeholder capabilities to address these needs will require:

**a. Government Support and Planning for National Scale Emergency Power**

Local, state and Federal emergency management planners, in coordination with private sector stakeholders, will need to address backup generation shortfalls for critical facilities in three key areas.

**i. Expanded National Emergency Generator Inventories:** Existing stocks of emergency generators (including those in FEMA’s Power Packs and those available on the private market) are marginally adequate to meet requirements in hurricanes and other limited-scale events. For multi-region, long duration outages, these inventories will fall far short of need.

Emergency managers should collaborate with industry to acquire adequate, regionally-distributed supplies of Black Sky hazard-protected emergency generators, with generator sizes and overall inventories configured to respond to anticipated regional needs. This coordinated government effort should also include considerations for pre-planned production and national-scale distribution of emergency diesel fuel, as well as transportation security planning for this distribution.

---

ii. **Black Sky Certification for Selected Fuel Providers:** The continued availability of fuel for this emergency generator inventory will be critical in long duration events. Selected, regionally-distributed diesel fuel suppliers and distributors should be identified and, with government encouragement, self-selected to develop and implement Black Sky Playbooks to ensure their operational capability in such severe hazard scenarios.

iii. **Transportation Security:** Emergency generator delivery and fuel re-supply operations may need to take place in a severely disrupted transportation environment. Black Sky transportation security planning will be necessary to ensure relevant public and private sector partners can develop and implement adequate processes to secure essential thoroughfares for generator and fuel distribution.

b. **Industry-Government Planning for Resupply of Essential “Consumables”**

Equivalent initiatives to deal with supply chain disruption will be needed for consumable supplies and resources necessary for sustaining infrastructure operations, such as treatment chemicals for major city water systems. The POIA identifies further supply chain and logistical risks that Black Sky Playbooks will need to take into account.

Failure to deliver essential emergency supplies will cripple Black Sky emergency operations. As part of broader, cross-sector efforts to prioritize and fully implement Black Sky operations, industry and government stakeholders should identify the supply chains (and components thereof) that deliver the most critical consumable supplies and resources for Black Sky sustainment and restoration activities. This identification process will be essential for companies that help provide food, pharmaceuticals, and other supplies necessary to sustain affected populations. However, a broad range of other supply chains will also be vital for resilience against


Black Sky events, including critical spare parts for replacing damaged infrastructure components, fuel for emergency power generation, and other emergency operational needs.

To help ensure that these supply chains can survive and function as required, it would be valuable if industry and government could partner to create a “Black Sky certification process.” DHS and FEMA should collaborate with infrastructure owners and operators to develop a set of government-based incentives and decision criteria to provide for this certification. Participating suppliers – ideally regionally-distributed to ensure national coverage – would agree to develop and adopt a Black Sky playbook, acquire and maintain adequate emergency generation capabilities, and ensure that their personnel have Black Sky-specific training. These providers will also need to acquire a Black Sky Emergency Communication and Coordination (BSX™) node, as examined further in Chapter II, to provide for communications and coordination capabilities in severely disrupted environments.

c. Regulatory Relief and Cost Recovery

In many cases, these initiatives will require regulatory relief and provisions for cost recovery. Building consensus between regulators, emergency managers, legislators, and other resilience stakeholders will be essential to fund the targeted resilience initiatives necessary for Black Sky preparedness. Including all relevant stakeholders in the Playbook development process can help build such consensus. Their participation in multi-sector exercises such as EARTH EX can also raise awareness of the need for investments in critical inventories and distribution system improvements.37

---

B. Complex Cross-Sector Interdependencies: The Emerging System of Systems

The growing interdependency between infrastructure and resource sectors will create additional challenges for sustaining and restoring critical infrastructure in Black Sky events.

Three problems are especially notable.

1. Cascading effects created by the failure of one sector on many others.
2. The risk that interdependent sectors will cause mutually-reinforcing failures.
3. Difficulties of predicting how such failures will occur, given the increasingly complex and tightly-coupled linkages between sectors – including those vital for supporting incident response operations.38

1. Cascading Failures: Electricity, Communications, and Beyond

Emergency managers have long been aware of the dangers posed by the cascading failures that breakdowns in transportation systems can inflict on other sectors, such as the supply of food, liquid fuels and other essential commodities for incident response. These dangers are especially significant in major urban areas. For example, approximately 95 percent of New York City’s food travels into the city by truck, and does so via a limited number of access points (mainly bridges). In fact, an estimated 30 percent of the truck traffic over the George Washington Bridge on

any given day carries food.\textsuperscript{39} Strengthening the protection of the Hunts Point Food Distribution Center against flooding will be of limited benefit if natural or manmade events disrupt these transportation choke points, or halt the electric and water utility service on which the Center depends.

George Washington Bridge: 95\% of NY City food is brought in by truck.

In addition, the dependence of all infrastructure sectors on electricity and communications make those two industries a prime risk factor for cascading failures. Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, identifies communications and energy infrastructure as “uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.”\textsuperscript{40}

That criticality is growing. It is only a slight exaggeration to conclude that the United States is undergoing “the electrification of everything.” The replacement of gasoline-fueled vehicles with ones relying on electricity is only a small part of a much larger transformation in the United States and abroad.

\textsuperscript{39} The City of New York, A Stronger, More Resilient New York, June 2013, p. 223.
In manufacturing operations and industrial activities across the economy, electric drives are replacing mechanical drives and motors fueled by other energy sources at an accelerating rate.41 Electric drives tend to be much cheaper to manufacture and maintain. They often perform more efficiently, and in many cases, produce lower net environmental emissions, even accounting for the emissions produced by generating the electricity they require.42 However, these compelling advantages come at the price of magnifying the cascading infrastructure failures that Black Sky power outages will create, and the scale of societal catastrophe and economic disaster the United States would suffer as a result.

The networked communications, sensors, and control systems provided by the Internet of Things (IoT) pose a similar mix of irresistible benefits and significant risks.43 An estimated 50 billion devices will be connected to the Internet by 2020.44 Even today, this vast network has already become absolutely

The Internet of Things (IoT) has become essential to societal functionality. Coordinated planning to replace a small portion of that functionality is a key requirement for Black Sky resilience.

---


43 The IEEE Standards Association defines the Internet of Things (IoT) is a system consisting of networks of sensors, actuators, and smart objects whose purpose is to interconnect “all” things, including every day and industrial objects, in such a way as to make them intelligent, programmable, and more capable of interacting with humans and each other. See: The Institute of Electrical and Electronics Engineers, IEEE-SA Internet of Things (IoT) Ecosystem Study, 2015, http://www.sensei-iot.org/PDF/IoT_Ecosystem_Study_2015.pdf.

essential to the normal functioning of society. It also lies at the heart of the emerging smart grid and the efficiencies it provides. One of the key challenges of Black Sky resilience will therefore be developing coordinated, robust multi-sector plans that can partially replace the functionality of the IoT during a long duration, multi-region blackout.

This proliferation of connectivity also creates new challenges for defending U.S. critical infrastructure from cyberattacks. The IoT generates new attack surfaces for adversaries to exploit and enables cyberattacks on physical components of critical infrastructure systems that were not previously connected to such vulnerable networks.

The IoT can also help adversaries greatly magnify the effectiveness of existing means of attacks against the electric grid and other sectors. Botnets offer a prime example. In 2016, the “Mirai” botnet attack used IoT devices, including baby monitors, to create the largest distributed denial-of-service attack in history. Adversaries manipulated IoT devices in foreign countries to collectively attack a U.S. company. The Department of Energy emphasizes that the Mirai attack “underscores the national security and economic vulnerabilities associated with the growing proliferation of unhardened consumer devices on the distribution network that have the potential to infect bulk power systems.”

DOE and its electric industry partners are addressing these cyber risks as a key challenge for subsector resilience. However, the IoT and its associated vulnerabilities are spreading across transportation, healthcare, and other sectors as well. A growing number of these IoT-connected sectors are also tightly-coupled: that is, these sectors have prompt and major impacts on each other when disruptions occur. As with the smart grid, this IoT connectivity can achieve extraordinary efficiencies and cost savings in multi-sector infrastructure.

---


operations. But increasingly complex dependencies and tight coupling also exacerbate risks of cascading failures. This connectivity can also create novel failure modes for adversaries to exploit – for example, by manipulating the demands for power in multiple, large-scale buildings and other loads to create grid instabilities.

These risks from the Internet of Things are not hypothetical or remote. Admiral Michael S. Rogers, the Commander of U.S Cyber Command, notes the IoT is already providing “millions of new Internet-connected devices for adversaries to exploit.” Those exploitation opportunities will continue to grow:

Today, consumers who can hardly keep up with patching their laptops and updating their cellphone operating systems are wondering how to upgrade the firmware on their home security cameras or Wi-Fi extenders to keep their families and homes from being victimized by malicious cyber actors. Technological developments are outpacing laws and policies, and indeed will have long-term implications that we have only begun to grasp.

The October 2017 release of “KRAK” (Key Reinstallation Attack) malware, used against wireless encryption systems for IoT devices, constitutes just the first wave of the attacks to come. Kevin Fu, computer scientist at the University of Michigan, notes that “For the general sphere of IoT devices, like security cameras, we’re not just underwater. We’re under quicksand under water.” The resulting risks to infrastructure resilience expand beyond particular sector-specific classes of devices; an attack on one sector could disrupt many others, given the tight interconnectivity between them.

---

Finding

The United States is not prepared for the resilience challenges posed by increasing cross-sector vulnerabilities.

The electrification of everything, the rise of the Internet of Things, and other sources of cross-sector connectedness have outstripped efforts to understand and mitigate the security problems these trends create. Aggressive policy and technology initiatives will be required to address such challenges. Infrastructure owners and operators and their government partners will also need coordinated, resilient multi-sector plans to partially replace the functionality of the IoT during a Black Sky outage in order to provide for societal continuity.

New device-level and IoT-wide security options are emerging to help address IoT cyber challenges. In the meantime, infrastructure owners and operators must expect that adversaries will exploit growing cross-sector vulnerabilities to exacerbate the difficulty of sustaining and restoring critical services in Black Sky events.

Recommendation: Develop exercises to reveal emerging interdependencies and facilitate the inclusion of cross-sector mitigation measures in Black Sky Playbooks.

In 2017, the inaugural exercise of the annual EARTH EX™ series examined cross-sector resilience for Black Sky hazards. Over 3000 participants, including more than 500 agencies and organizations, as well as 16 infrastructure, NGO and government sectors spanning 14 nations, were involved. In GridEx, the premier, biennial electric subsector exercise conducted by the E-ISAC, exercise scenarios and play include a growing focus on communications, gas, financial services, and other systems to identify mutual support requirements.


Owners and operators are expanding their attention to cross-sector disruptions as well. The Hamilton exercise series, led by the financial services sector, held a joint exercise with electric subsector participation and communications sector observers in August 2016.52

The Department of Homeland Security’s Cyber Storm exercise series includes a focus on cross-sector coordination, with the most recent iteration – Cyber Storm V – including participants from the communications, public health, commercial facilities, and information technology sectors.53 Cross-sector exercises involving the electric and oil and natural gas (ONG) subsector, including Liberty Eclipse (December 2016), are also growing.54

Going forward, exercises in these and other sectors should be specially designed to identify emerging gaps in cross-sector resilience and to assess the viability of new plans for addressing those shortfalls.

2. Smart Cities Automation and System Autonomy

New cross-sector vulnerabilities will have their greatest impact in “Smart Cities.” DHS defines Smart Cities as “urban centers that integrate cyber-physical technologies and infrastructure to create environmental and economic efficiency while improving the overall quality of life.”55 Smart Cities are using technology to manage energy, transportation, and manufacturing systems, and using increasingly automated technology to monitor these systems and improve efficiency.56

These developments also create new risks of cascading failures. Greater demographic concentrations will also increase the impact of such failures, compounded by the likelihood that many citizens within these urban centers

will be economically unable to conduct any emergency preparedness activities. With the accelerating adoption of smart technologies in dense urban areas and the tight connectivity they enable between infrastructure components, the dependence of Smart Cities on these increasingly complex systems will necessitate specialized efforts to strengthen their security.

However, DHS warns that “Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.” Given the increasing concentration of essential commodity distribution nodes in a dwindling number of cities, these Smart City vulnerabilities will exacerbate the difficulty of sustaining and restoring critical services in Black Sky events. Those vulnerabilities also heighten the urgency of developing new approaches to provide situational awareness within Smart Cities, as well as modeling tools that can use such data to help secure them, and guide response and restoration operations when disasters occur. Emerging new capabilities to address this need, including the Global Infrastructure Network Optimization Model (GINOM™), are reviewed later in this Handbook.

Still deeper changes in the emerging infrastructure system of systems are on the horizon. In a path-breaking work on cross-sector vulnerabilities, Michael Assante and Andrew Bochman examine the “massive deployment of increasingly automated and even autonomous systems” that is underway, and highlight the risks that this accelerating (and seemingly unstoppable) trend will create for catastrophic infrastructure breakdowns in New York City and megacities around the globe.

---

59 Michael Assante and Andrew Bochman, "IoT, Automation, Autonomy, and Megacities in 2025: A Dark
A number of initiatives are underway to strengthen resilience in major urban areas. The Rockefeller Foundation’s ‘100 Resilient Cities’ (100RC) initiative is the most prominent and far-reaching of these efforts. 100RC is aggregating information on the evolving demands of resilient cities, and “signals to the private sector what tools and services cities need.” The initiative is also designed to help cities sustain critical services regardless of the chronic stresses and acute shocks they experience.

However, the 100RC effort does not examine the risks posed by catastrophic events and the cascading infrastructure failures they would create. Nor does the initiative recommend measures to deal with the new vulnerabilities created by the rise of Smart Cities, or the rise of increasingly automated, tightly-coupled infrastructure systems.

Finding

The rise of smart megacities in the United States and partner nations is creating serious challenges for cross-sector resilience.

Over and above the broader fragilities created by increasingly complex, automated, and tightly-coupled infrastructure systems, the growth of megacities creates special problems for Black Sky preparedness. The 2017 hurricane season highlighted the degree to which expanding urban areas in the continental United States remain in the path of severe weather events. EMP, coordinated cyber-kinetic attacks, or other Black Sky hazards, will create vastly greater risks of cross-sector disruption in such cities and the surrounding regions that depend on them.

---

61 Ibid.
62 ARUP, City Resilience Index, December 2015, pg. 7. The City Resilience Index (CRI), created as a tool to measure and monitor factors that contribute to overall resilience, emphasizes the need for “continuity plans to maintain utility services to critical assets during emergency situations.” But the CRI does nothing to define an emergency situation, nor make any suggestion as to how cities are to build resilience against catastrophic events.
**Recommendation:** *Make smart megacity infrastructure resilience a special focus for Black Sky Playbooks and exercises.*

Urban planners and city managers should be included in Black Sky planning and exercises to ensure that they account for the risks of adopting smart city technologies. This expanded effort should also include collaboration with leading infrastructure owners and operators who will be required to sustain megacity populations and critical functions in Black Sky events. Such collaboration should also go forward on a multinational basis, given the degree to which many of the United States’ international partners are experiencing explosive growth in their own urban areas.

3. **Mapping Systemic Risks, and Implications for Black Sky Response Operations**

Multi-sector planning and real-time decision-making for Black Sky hazards will be enormously complex. Charles Perrow, who pioneered the analysis of failures in such tightly-coupled systems, notes that because of the growing complexity and connectivity within and between infrastructure sectors, “We have produced designs so complicated that we cannot anticipate all the possible interactions of the inevitable failures.”

Even as modeling tools and technologies improve, tightly-coupled infrastructure will produce unanticipated cross-sector failures.

The expanded use of automated and autonomous control systems in interdependent infrastructure sectors will create still further impediments to attempts by decision makers, without appropriate guidance, to predict how they will affect each other. DHS also notes that the introduction of Artificial Intelligence to control infrastructure systems and manage their interactions will introduce further uncertainties for understanding and mitigating risks of cascading infrastructure failures.

---


Despite these challenges, modeling cross-sector interdependencies will be essential for efforts to mitigate their catalytic role in catastrophic infrastructure failures. Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (February 2013), emphasizes the need to “anticipate interdependencies and cascading impacts.” To help achieve this goal, the National Infrastructure Simulation and Analysis Center (NISAC) and the Office of Cyber and Infrastructure Analysis (OCIA) lead cross-sector modeling and analysis for the Department of Homeland Security. The NISAC uses advanced modeling, simulation, and analysis capabilities to provide policy guidance to both government and industry by mapping complex interdependencies between sectors and evaluating the vulnerabilities they create. The NISAC and OCIA are also developing an Urban Interdependencies Model to assess cross-sector vulnerabilities in major cities and has models to examine supply chain disruptions in several areas including transportation fuels and chemicals.

The NISAC also conducts analyses of threat-specific risks to infrastructure. In advance of a major hurricane, for example, the Center can provide data about the possible consequences of that event for local and regional infrastructure. In the event of a major cyberattack that disables power over a wide area, the NISAC will also seek to assess the potential impact of that attack on other sectors and on the U.S. economy. Such threat-specific analysis could be enormously valuable for supporting infrastructure sustainment and restoration operations in Black Sky events.

---


The Regional Resiliency Assessment Program (RRAP) provides another DHS-led initiative that can help map cross-sector interdependencies and share that information with a broad array of government and private sector partners. RRAP projects analyze data on critical infrastructure within designated geographic areas, concentrating on issues that could have regionally and nationally significant consequences. Infrastructure owners and operators can use the Resiliency Assessment and key findings to guide strategic investments in equipment, planning, training, and resources to enhance the resilience and protection of facilities, surrounding communities, and entire regions.\textsuperscript{69} DHS is also continuing to enhance its IP Gateway system as a “usable repository of cross-sector critical infrastructure information and a source of understanding key dependencies.”\textsuperscript{70}

Ensuring that this collection of data keeps pace with rapid infrastructure changes will be particularly critical. To maintain the accuracy of interdependency assessments and support public and private sector resilience initiatives, infrastructure owners will need to continually provide DHS with updated data on the evolution of their supply chains, consolidation and “leaning” initiatives, and further initiatives to seek efficiencies by increasing their reliance on other sectors and the IoT. But much of this data will be proprietary and highly business-sensitive. Regulatory and antitrust concerns may also create challenges for sharing information with DHS (and between companies within specific sectors) to support cross-sector modeling and analysis.

However, Black Sky threats create an urgent need for modeling capabilities beyond static interdependency assessments of key sectors. Given the inevitable complexity facing decision makers in these catastrophic events, industry and government leaders will need a dynamic, real-time infrastructure and supply chain simulation model that spans all relevant infrastructure, resource, and service supplier sectors. Such a simulation model will have to account for the reach and response opportunities of emergency responders, and for critical supply chains which are increasingly global in scope.


One promising approach to meet these modeling requirements is to use a building block methodology: that is, to build models of specific infrastructure components and their key interdependencies, then integrate them to provide an overarching model. But that integrative effort will entail enormous complexities. To facilitate integration, the model could use advanced agent-based techniques that focus on sector interfaces and limit requirements for real-world, proprietary data from infrastructure owners and operators.

EIS Council has begun hosting a multi-sector, international team to build such a model. The Global Infrastructure Network Optimization Model (GINOM™), now in an early stage of development, is focused on providing a real-time, multi-sector simulation that can be used to support both pre-event and crisis decision-making. The development team includes some of the largest utility corporations in the world, along with multi-sector domain knowledge specialists, infrastructure modeling experts, and relevant academic institutions. In the coming months and years, the GINOM™ and similar initiatives may provide a unique opportunity to address critical modeling and simulation needs. Another promising initiative, SpatialOS, is beginning to test the application of these modeling and simulation capabilities. The platform is being piloted in a select number of use cases to assess the consequences, including cascading effects, of infrastructure design and investment.71

**Finding**

*Improved mapping and modeling of sector interdependencies to inform resilience planning is vital. Real-time simulation spanning all critical infrastructure sectors and supply chains will also be essential for Black Sky sustainment and restoration operations.*

Identifying critical requirements for cross-sector support and potential sources of cascading and mutually-reinforcing failures is difficult, and yet absolutely essential for Black Sky hazards. Those difficulties are magnified by the need to continuously update such vulnerability assessments as sectors continue to modernize, and by the business and security sensitivity of the data.

---

required to support accurate cross-sector modeling. To provide adequate, real-time decision-making guidance, an evolving simulation model spanning all U.S. infrastructure sectors and key international supply chains will be required.

**Recommendation:** Leverage available interdependency vulnerability models to formulate cross-sector support plans and develop real-time infrastructure simulation models for decision support in Black Sky events.

To improve U.S. capabilities for addressing complex catastrophes, infrastructure owners and operators and their government partners should leverage available infrastructure interdependency expertise and modeling, especially the capabilities resident at DHS. This modeling data should also guide resilience policy planning and decision-making. In addition to the DHS-sponsored modeling efforts described above, many sector-specific Information Sharing and Analysis Centers (ISACs) have made progress in overcoming modeling challenges within their own sectors. These ISACs should expand their emerging work on cross-sector resilience issues and consider sustained data support to the National Infrastructure Simulation and Analysis Center and the Office of Cyber and Infrastructure Analysis. Infrastructure owners and operators should also examine how the Protected Critical Infrastructure Information (PCII) Program and other existing information sharing initiatives could be supplemented to deal with emerging data requirements for infrastructure mapping and modeling.\(^2\)

However, developing adequate “machine support” for real-time, multi-sector decision-making during a Black Sky event will require an evolving multi-sector simulation capability. The Global Infrastructure Network Optimization Model (GINOM\(^{TM}\)) represents a unique example of such a simulation that can build on interdependency assessment initiatives in especially valuable ways. Simulating “complex adaptive systems,” the project leverages recent advances in tools to model large-scale networks of interactive systems. These tools work by recognizing that the dynamic, changing “states” of component subsystems result in emergent and very different behaviors of the overall system. Rather than trying to construct complex, static models of high-level entities,

algorithmic representations of the rules relating the entities’ comparatively simple components simulates the changing interactions of those components, allowing the dynamic behavior of the overall entity to emerge. Public and private sector stakeholders involved in preparing their sectors for complex catastrophe scenarios should foster the development of this new AI-based capability.

C. Threats to Cross-Sector Resilience: The Strategic Challenge

The changing architecture of U.S. infrastructure accounts for only part of the challenge of building Black Sky preparedness. At the same time that many sectors are becoming increasingly fragile and interdependent, manmade threats to infrastructure are becoming increasingly severe. Earthquakes and other catastrophic natural hazards also create immense risks to cross-sector resilience. These threats will heighten the need to prioritize the sustainment and restoration of critical services and will require new forms of industry-government and cross-sector collaboration.

1. Natural Hazards

Recent hurricanes have highlighted the risk that natural hazards pose to cross-sector resilience. When Hurricane Maria struck Puerto Rico, all lifeline sectors broke down at once. As noted by Puerto Rico’s Director of Safety and Protection, “everything collapsed simultaneously.”

Recent exercises have also highlighted the imperative to embed Black Sky-compatible infrastructure sustainment and restoration operations into the heart of incident response plans and coordination mechanisms. The 2016

---

Clear Path IV and Cascadia Rising exercises offer particularly valuable insights. Both exercises were based on the scenario of a 9.0 magnitude earthquake and subsequent tsunami striking the Pacific Northwest.

Earthquakes of that severity will put a premium on rapid restoration of critical infrastructure services. Washington State’s after-action report (AAR) from Cascadia Rising determined that once the earthquake strikes, and electric service, food distribution, waste removal, and other lifeline services are disrupted, “the clock is ticking to a humanitarian disaster.”

The AAR found that emergency managers can help stave off mass casualties by having DOD and other Federal agencies immediately “push” assistance to the affected states, rather than waiting for state authorities to request (or “pull”) such assistance via the processes typically used in incident response. The Review found that “due to the wide spread damage, sense of urgency, and barriers to normal communication and coordination” in catastrophes, the traditional pull system would be “grossly inadequate.” Instead, “Preplanning the ‘first wave’ of life saving resources and their movement and delivery all the

---


75 Ibid.
way forward” to the stricken area, “absent any request, is key.”

This proactive approach will also be useful in a broad range of other natural and manmade Black Sky events.

But even with extensive pre-planning, the delivery of emergency resources can never offer more than a stop-gap solution for saving lives in Black Sky events. Earthquakes and other catastrophes will inflict extensive damage to transportation infrastructure essential for executing delivery operations. Water deliveries to urban areas with millions of inhabitants, as opposed to Flint (Michigan) scale operations, will be enormously difficult to sustain. The disruption of wastewater and sanitation services present still greater problems for emergency managers, given the risks of disease that will rapidly emerge. Power outages will also create cascading failures across a broad array of other electricity-dependent facilities and functions. For example, telecommunications connectivity, which is often taken for granted, will cease to function in a wide area, long-term outage. Without power, many facilities, including healthcare services, will also be forced to shut down as emergency power generators break down and diesel fuel stocks fall drastically short of need.

Mass evacuation provides one option to prevent extensive casualties as resupply operations falter. However, former FEMA Administrator Craig Fugate argues that this option is impractical for New York City and other major urban areas. With so many people to evacuate, “[you] can’t move ‘em fast enough.” Evacuating such a large city would be even more difficult in a Black Sky event due to the disruption that such an event would inflict on road, rail, and air transportation, and still more challenging without the availability of effective, widely-distributed communications. Moreover, while Fugate dismisses the viability of evacuating even a single metro area as impractical, multiple cities across entire regions of the United States could be in similar need of evacuation in Black Sky events.

---

76 Ibid.
Mass evacuation can be challenging even in less severe disasters. In hurricanes Harvey and Irma (2017), the residents of Texas and Florida, respectively, received conflicting advice from different government officials. During Harvey, Texas Governor Greg Abbott urged people to “strongly consider” evacuating. Meanwhile, Houston Mayor Sylvester Turner emphasized that there would not be an evacuation warning, and suggested that residents might be in more danger by attempting to do so. In Florida, counties differed in their timing or decision to issue evacuation orders, but Governor Rick Scott was clear in telling those who planned to evacuate to "get out now." In both cases, those that chose to evacuate faced severe congestion on highways and other roads.

In a Black Sky event, the expansive affected area will leave no viable destinations for most people attempting to evacuate. A spokesman for Mayor Turner noted that the decision not to evacuate for Hurricane Harvey was in part influenced by the experience of Hurricane Rita in 2005, in which motorists ran out of fuel on the roads, and there were a number of deaths. This would likely occur on a vastly greater scale in Black Sky scenarios. And while evacuation

---


was feasible for some Texan and Floridian residents in the recent hurricanes, they were also afforded sufficient warning – which may not be available prior to many Black Sky events.

In lieu of mass evacuation, sheltering in place will be the most sensible strategy. Implementing the limited Black Sky infrastructure sustainment missions that many sectors are developing in EPRO Black Sky Playbooks will be particularly important. These Black Sky missions, where implemented, would provide at least minimal utility service and minimally sustainable levels of other critical services during the “power gap” – until electricity and other infrastructure services return to near-normal levels.

Prudent and prioritized investments in infrastructure resilience can also play an important role in reducing restoration times, enabling “shelter in place” and related strategies.

While significant prioritized investment should go forward for the most critical infrastructure assets and facilities, minor investments can also be beneficial. Florida Power & Light, for example, inspects poles for strength and upgrades wood poles to concrete or steel to prepare for storm season. Hardening this infrastructure, thereby reducing the need to clean up debris and maintaining paths required for restoring power, sped up response times in Hurricane Irma. Minor investments contributing to overall system hardening against natural disasters can have a great cumulative effect and help enable sheltering in place strategies to save countless lives.

**Finding**

*The most viable strategy to save lives when Black Sky hazards strike is to support infrastructure sustainment and restoration operations, while enabling shelter in place.*

---

Improved pre-planning to push water and other emergency commodities forward, including through the use of Pre-Scripted Mission Assignments, can help support initial efforts to facilitate sheltering in place.\textsuperscript{84} However, much broader cross-sector planning and resilience investments will be required to save and sustain lives in Black Sky events. These requirements include:

1. Targeted investments to harden facilities and functions essential for sheltering in place. Water systems and other lifeline infrastructure must be able to sustain minimal levels of service, as defined by utility operators, emergency managers, and other stakeholders. Prioritized investments to protect the most critical facilities and systems can improve their odds of surviving Black Sky events.

2. Pre-planned support for sustainment and restoration operations. Each sector will need to identify external requirements for Black Sky sustainment and restoration operations, and collectively pre-plan the coordinated provision of these essential services with critical partner sectors and emergency response organizations. This coordinated, cross-sector mutual support will be essential for both sustaining surviving infrastructure and for accelerating the complex restoration of water, wastewater, electric utilities, and other essential commodities and services.

Despite ongoing improvements in executing these strategies, mass casualties will likely be unavoidable in many Black Sky scenarios. Public health officials will also need to plan and prepare for significantly expanded support to mortuary services in catastrophic events, including the deployment of Disaster Mortuary Operational Response Teams (DMORTs).\textsuperscript{85}

\textit{Recommendation. DHS, FEMA and their state and local partners should put infrastructure operations at the heart of incident response planning and management.}


Section V will provide detailed recommendations to better integrate infrastructure sustainment and restoration operations with broader incident management. However, the first step to do so is to involve emergency managers in the development of Black Sky Playbooks for essential infrastructure, service and resource sectors.\textsuperscript{86}

Emergency managers can leverage the expertise of infrastructure owners and operators, particularly with regards to identifying what supplemental services will be needed to support their sector’s sustainment and restoration operations in Black Sky events. These managers can also ensure that infrastructure owners and operators in each sector incorporate partner sector and national security priorities into their Playbook development efforts.

Emergency managers can also help maximize the number of survivors able to shelter in place during Black Sky outages by effectively facilitating mass shelters. Although mass shelters cannot be the primary answer for such hazards, they will be absolutely essential to enable shelter in place strategies. Ensuring that these shelters have the infrastructure services they need to assist displaced survivors will particularly vital. Such efforts will require close coordination with NGOs that have primary responsibility for mass care. The FEMA regional planning framework outlined in the POIA will provide an especially useful mechanism to integrate such efforts.

**Finding**

*Mass evacuation in Black Sky events is impractical and will exacerbate the challenge of providing critical infrastructure services to the public.*

For most people affected by multi-region catastrophes, there will be no viable destinations for evacuation. Sheltering in place will be the best option in most Black Sky events.

However, several challenges remain to sheltering in place effectively. Without electricity, homes will not have heat in winter, or cooling in the summer. Houses will also be without refrigeration. Without crucial support from emergency

---

\textsuperscript{86} The expanding, EIS Council-hosted EPRO\textsuperscript{®} SECTOR process represents a particularly focused example of such playbook development. See: “E-PRO\textsuperscript{®} SECTOR Project,” EIS Council, n.d.,a, http://www.eiscouncil.org/EPro/Esc.
management stakeholders to provide emergency fuel and treatment chemicals, there may be, at best, non-potable water service, and likely no wastewater services. Indeed, individual homes are unlikely to be among the priorities for sustained infrastructure service in Black Sky outages. Mass shelters provide a potentially more effective alternative. However, with current, limited levels of planning for such crises by relevant stakeholders, residents are unlikely to have any information about these shelters and other critical issues due to a lack of communications capabilities. Local law enforcement operations may also be severely disrupted, at a time when the risk of looting or other crimes may be heightened. Nevertheless, these challenges will pale in comparison to the difficulty of providing services to stranded individuals and families who tried and failed to evacuate.

**Recommendation:** *Federal, state and local government officials, in coordination with private sector partners and NGOs involved in “whole community” preparedness, should improve plans and capabilities to enable sheltering in place.*

Enabling affected citizens to shelter in place will require, at minimum, careful, coordinated planning to ensure basic levels of continued service from lifeline sectors, e.g., potable water or support for treatment of non-potable water. Achieving these minimum essential levels of service will require significant pre-planning efforts and Black Sky preparation by critical infrastructure sectors and selected segments of their critical supply chains.

As part this planning, special attention will also be needed for institutions and communities where particularly vulnerable segments of the population are under the care of others, such as schools and daycare, hospitals, prisons and jails, and elder care.

Plans for sheltering in place should also draw from the POIA’s analysis on mass care and emergency services.\(^{87}\)

---

2. Manmade Hazards and Geomagnetic Disturbances (GMD)

Manmade threats will pose many of the same cross-sector resilience challenges as natural hazards. As with earthquakes or catastrophic storms, adversaries can be expected to strike multiple infrastructure sectors at the same time, rather than simplifying U.S. response requirements by attacking only one. Manmade threats may also be at least as challenging in terms of geographic scope. While it is conceivable that adversaries might launch a small “demonstration” attack early in a severe crisis, or otherwise constrain the scale of their strike, attacks could also occur on a vastly larger scale. An attack with a single High Altitude Electromagnetic Pulse (HEMP) could disrupt power grid components (and the microelectronics on which all other infrastructure sectors depend) over a third of the United States or more. Moreover, any adversary with HEMP capabilities may be likely to launch multiple simultaneous strikes. Adversaries could also conduct cyberattacks and targeted kinetic strikes across the entire nation, potentially inducing knock-on effects that affect U.S. partners and allies.

Yet, manmade threats also differ from natural hazards in key respects. In contrast to Mother Nature, adversaries will strategically target U.S. infrastructure. Attackers can seek to capitalize on the trends in infrastructure

---

fragility analyzed in the previous section, and exploit interdependencies to maximize the disruption of U.S. national security, the economy, and public health and safety. Adversaries can also combine their attacks with information warfare operations to incite panic and corrode public confidence in the U.S. government’s ability to defend the nation.

The threats examined in EPRO Handbook Volume I have continued to intensify since its publication in December 2014. Infrastructure owners and operators have responded by ramping up their investments in system protection and restoration, particularly against cyber and physical threats. However, progress to date has been uneven across sectors, and among utilities within the sectors.

For the threats these particularly challenging hazards pose to today’s hyperconnected infrastructure sectors, cross-sector resilience will be essential. Yet, preparing the key elements needed to support such resilience will require additional initiatives. The sections that follow highlight recent increases in manmade threats to critical infrastructure and examine the implications for government-industry collaboration to sustain and restore essential services when attacks occur.

**a. Electromagnetic Pulse (EMP)**

The U.S. Department of Defense is taking new preparedness measures to manage the risk that North Korea or other potential adversaries will use their expanding nuclear programs to produce and use EMP devices. Most notably, U.S. Northern Command (responsible for defending the U.S. territory) has shifted communications equipment and other critical systems to Cheyenne Mountain in Colorado, which, “because of the very nature of the way that Cheyenne Mountain is built,” is “EMP-hardened.”

---

However, the U.S. Congress has expressed concern that such efforts are inadequate to address nationwide vulnerabilities to EMP threats. In the National Defense Authorization Act for Fiscal Year 2016, legislators noted that while DOD is hardening its own systems against EMP effects, the Department “relies heavily on civilian utility providers to meet installation energy requirements,” making the hardening of those civilian-owned systems essential for national defense.91

Significant progress is underway in some of the leading electric companies to plan and, in a few cases, build resilience against EMP attacks. A small but growing number of electric utilities are now using their own resources to invest in or plan for EMP protection. In particular, some utilities are selectively hardening control centers and other key system components, and adopting new filter technologies, current blocker systems, and shielding products to achieve increasingly cost-effective levels of protection.

Aggressive research is also underway to set the stage for further progress. EIS Council is collaborating with U.S. and international electric companies, the Defense Threat Reduction Agency (DTRA), and other partners on a range of research and development initiatives to support EMP resilience.

Key activities include:

- Ongoing EIS Council-sponsored EMP testing of high power relays, generator control systems, and other key grid hardware;
- EIS Council coordination with Israel Electric Corporation’s 3-year effort to build a full national grid EMP protection plan;
- EIS Council development of EPRO EMP – an EMP-focused handbook resource planned to include an updated summary of best-in-class EMP protection strategies and methodologies for all power grid elements, in the form of a user-friendly, voluntary specification;
- Development of new, cost-effective protection models, including supplemental shielding for especially critical relay, control, and communications devices; and
- Study efforts conducted by the Electric Power Research Institute (EPRI), Sandia National Laboratory and other research institutions to assess EMP vulnerabilities of high voltage transformers and other grid components, and to examine options for greater system resilience.\(^2\)

The Department of Energy is supporting such efforts with its January 2017 Electromagnetic Pulse Resilience Action Plan. The Plan lays out an aggressive set of initiatives to better understand the emerging threat, test and promote new approaches to mitigation and protection of electric infrastructure, and enhance grid response to (and recovery from) attacks.\(^3\)

The Action Plan builds on the Joint Electromagnetic Pulse Resilience Strategy (July 2016) developed by DOE, EPRI and other subsector partners. DOE also recently partnered with DHS’ National Protection and Programs Directorate for a joint study on EMP science and potential risks to critical infrastructure.\(^4\)


\(^4\) Brandon Wales, Testimony Before the United States House of Representatives Committee on Homeland Security Subcommittee on Oversight and Management Efficiency, May 17, 2016,
The communications sector also deserves credit for its ongoing hardening efforts. Specific examples of such efforts, and proposals for additional measures under the BSX initiative, are discussed in Chapter II.

Much, of course, remains to be done, as only a relatively small fraction of the nation’s electric subsector has begun efforts to implement EMP protection strategies. Progress is slower – and in many cases, virtually non-existent – in other critical infrastructure sectors. The failure of these sectors to keep pace with the intensifying EMP threat is understandable. For water utilities, transportation systems, and other sectors that received abysmal infrastructure resilience grades from the American Society of Civil Engineering, replacing aging system components constitutes an urgent and monumental task. Providing minimalist emergency power capabilities for water systems, key interstate gas stations, and other infrastructure assets poses a similar near-term challenge that can crowd out attention to other issues – especially those such as EMP that are relatively unfamiliar.

Nevertheless, these non-grid sectors are vulnerable to EMP effects. Use of microelectronics is ubiquitous across U.S. critical infrastructure. An EMP attack will not damage or destroy all such microelectronics; damage will occur on a probabilistic basis and will vary with system and attack-specific characteristics. But adversaries will be able to disrupt multiple infrastructure sectors with an EMP weapon, including water utilities and other systems vital for saving and sustaining lives in the aftermath of an attack. And, insidiously, they will damage electronic components of many emergency power generators as well.

Basic strategies for cost-effective EMP protection involve hardening core, regionally-distributed “backbone” elements of key sectors, especially the power grid, supplemented by the protection of critical, long lead

While some sectors are hardening against the EMP threat, many other utilities across all sectors are vulnerable to EMP effects, amplifying risks of cross-sector failures.
hardware that may be especially vulnerable. Combining such strategies with adequate pre-distributed spares, equipment testing, and a range of other supplementary measures would provide a foundation for the sustainment and rapid restoration of infrastructure systems following an EMP attack.

However, the vulnerability of multiple sectors to EMP will also create special challenges for cross-sector resilience. The initial U.S. focus on hardening the power grid against EMP attacks can help reduce cascading failures in other sectors. Implementing this focus will be essential to enabling relatively rapid restoration following wide area power outages triggered by an EMP attack. While, even under ideal conditions, such efforts would take days or weeks, this gradual process will be crucial to accelerating the restoration of power flows to communications systems and other critical electricity-dependent facilities and functions.

But hardening grid components will be near-useless if similar EMP protection strategies are only implemented in the electric subsector. Indeed, EMP hardening for natural gas systems and other infrastructure on which power generation and restoration depend will be particularly crucial, or the grid will remain vulnerable even as electric utilities improve the protection of their own components. Other critical infrastructure sectors should also develop plans to protect critical “backbone” hardware and unique long lead components from the effects of EMP and ensure an adequate range of pre-staged supplies and spares to support cross-sector resilience and infrastructure restoration.

b. Geomagnetic Disturbances

A geomagnetic disturbance (GMD) caused by severe solar weather could elicit similar consequences to EMP. Electrically and magnetically charged ejections of the sun’s coronal mass can cause significant variations in the earth’s magnetic field, producing geomagnetically induced currents. These currents can disrupt or damage electric infrastructure. A 2016 Executive Order acknowledged the potential for GMDs to cause multi-sector, cascading failures, and called for a plan to predict, protect against,
and respond to such an event. Government and industry leaders should maintain the momentum and progress afforded by this Executive Order, and incorporate efforts to build resilience against GMD into broader cross-sector resilience initiatives.

Finding

Hardening the grid against EMP and GMD provides only the starting point to build cross-sector resilience against such threats.

Infrastructure owners and operators and their government partners will need to take a holistic approach to ensure that not only is the U.S. electric system selectively protected from attack and/or natural hazard, but that the critical loads for population sustainment, disaster response, and national security will remain functional and be able to accept power. Congress has required the Secretary of Homeland Security to submit a strategy for protecting and preparing critical infrastructure against the threats of EMP and GMD. That strategy should explicitly focus on strengthening cross-sector resilience.

Recommendation: Industry, sector SSAs, and other resilience partners should begin long lead efforts to strengthen EMP/GMD resilience for all sectors.

The electric subsector and its government and research partners should ramp up sharing of their technologies and protection strategies for adaptation by other sectors. Given the importance of infrastructure survival to societal continuity and, in particular, to

Potential adversaries’ offensive cyber capabilities are improving – the most advanced of which far exceed the U.S.’s ability to defend key infrastructure.


national defense, the Department of Defense should also provide increased information on its emerging best practices with cleared infrastructure personnel.

c. **Cyber Threats**

Potential adversaries’ cyberattack capabilities are growing so rapidly that new cross-sector resilience strategies will be essential to safeguard public health and safety, the economy, and national defense. After a comprehensive review of the cyber threat to the United States and the efforts underway to strengthen the resilience of U.S. infrastructure, the Defense Science Board’s February 2017 report on cyber deterrence reached a key conclusion regarding the threat from major powers (e.g., Russia and China):

Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States’ ability to defend key critical infrastructures. 97

Other potential state adversaries are also improving their capacity to attack U.S. infrastructure. The Defense Science Board report found that “regional powers (e.g., Iran and North Korea) have a growing potential to use indigenous or purchased cyber tools to conduct catastrophic attacks on U.S. critical infrastructure.” 98 Moreover, challenges to cyber resilience posed by both state and non-state actors are intensifying across the full array of infrastructure sectors. 99

Cyber threats to the power grid pose special challenges for cross-sector resilience. DOE’s recent Quadrennial Energy Review 1.2 (January 2017), emphasized that the U.S. electric system faces “imminent danger from

---


cyber attacks.” Such attacks could offer adversaries special advantages because of the cascading failures they would create. The DOE Review warns that “Widespread disruption of electric service because of a transmission failure initiated by a cyber attack at various points of entry could undermine U.S. lifeline networks, critical defense infrastructure, and much of the economy; it could also endanger the health and safety of millions of citizens.”

The growing reliance of U.S. power generation on natural gas creates another avenue for cyber adversaries to cripple the grid and create such cascading failures. Indeed, given the increasingly complex dependencies between multiple U.S. infrastructure sectors, we should assume that adversaries will seek to leverage those interdependencies by launching multi-sector attacks. Moreover, each of the sectors that could be targeted in such an attack, including water and wastewater utilities, oil and natural gas systems, financial


services companies, communications systems, and their nodes of connectivity are facing increasingly severe, system-specific threats.

Infrastructure owners and operators are accelerating efforts to bolster the cyber resilience of their systems. However, new initiatives will also be necessary to meet the risks of cross-sector disruptions, and to help coordinate and prioritize cyber response operations for interdependent systems. The Federal government has recently taken a major step forward to help achieve such coordination between Sector-Specific Agencies. The December 2016 National Cyber Incident Response Plan (NCIRP) provides the “basis for national cyber operational playbooks” and operational coordination plans. However, the NCIRP does not itself provide such plans. The document offers only a strategic framework to help do so. Moreover, while the NCIRP provides a much-needed mechanism for coordination among Federal Departments, the Plan offers few details on how infrastructure owners and operators would help guide cross-sector response operations.


107 Ibid.

Finding

The NCIRP provides only a necessary first step towards broader cross-sector resilience.

Industry and government will need coordinated, multi-sector operational pre-planning and real-time engagement beyond current NCIRP guidance to weather a severe cyberattack on critical infrastructure with multi-region or nationwide consequences.

The owners and operators of critical infrastructure will need to play a leading role in defending and restoring their own systems from cyberattacks. Federal Sector-Specific Agencies (SSAs) can help them do so by providing real-time threat information and other types of support.

Accordingly, the NCIRP’s mechanisms to coordinate SSA operations across the Federal government will be valuable in cross-sector attacks and can provide a centralized Federal point of connectivity for private sector engagement. Federal support to envisioned multi-sector coordination structures will also be essential for restoration support and population sustainment in the aftermath of a widespread, catastrophic cyberattack on critical infrastructure. But owners and operators will need to build their own coordination mechanisms to make use of this connectivity, and to help build the operational plans that the NCIRP facilitates but does not provide.

Government support at the SLTT levels will also be essential. Relevant SLTT authorities will need to determine how best to feed into the Federal support system, and how to interface with infrastructure owners and operators.

Recommendation: Infrastructure leaders should create a Cross-Sector Coordinating Council (CSCC) to support broader cross-sector operational planning and coordinate incident response activities.

Section IV of this chapter will examine how the proposed CSCC can leverage existing coordination mechanisms, especially the Strategic Infrastructure Coordinating Council initiative,109 to meet the operational

---

requirements for cross-sector collaboration. While primarily engaging with government at the Federal level, in time, the CSCC should expand to include coordinated engagement with SLTT representatives.

d. Combined Attacks and Hybrid Warfare Campaigns

Ongoing government-sponsored studies are highlighting the risk that adversaries may combine cyberattacks with other means of striking U.S. infrastructure and then disrupting efforts to restore it.\(^{110}\) Two additional threat vectors could pose special challenges for cross-sector resilience against such combined, “hybrid warfare” operations: kinetic attacks and information warfare.

The electric subsector provides a starting point to examine cross-sector vulnerabilities to kinetic threats. The April 16, 2013, attack on the Metcalf electricity substation near San Jose, California highlighted the risk that state and non-state adversaries can use high powered rifles and other readily-available weapons to attack critical transformers.\(^{111}\) The North American Electric Reliability Corporation (NERC) responded by developing an array of physical security requirements to help protect substations and other key assets.\(^{112}\) However, adversaries can be counted on to seek kinetic attack options that circumvent enhanced security measures.

---


The use of unmanned aerial vehicles (UAVs) to employ explosives or use other means to damage and destroy equipment inside even protected substations offers a prime example of such adaptivity.113

A further risk is that adversaries will use kinetic attacks to disrupt sustainment and restoration operations. If attackers have the willingness and expertise to shoot transformers sited in remote substations, they may also seek to shoot replacement transformers as trucks, rail cars, and barges slowly move them to where they are needed (potentially across multiple states).

Utilities have detailed and well-exercised plans to use local law enforcement and contractor personnel to provide for safe transformer movement in peacetime conditions. A growing number of utilities also have plans to ensure the security of workers who might need to deploy to substations to support emergency operations in a cyberattack. However, if even a single “active shooter” event was to occur in conjunction with a cyberattack, vastly expanded security plans and capabilities would be required to support power restoration operations.

Even false social media reports that such shootings had occurred could disrupt efforts to restore electric service. Hurricane Katrina illustrated how false reports can disrupt incident response operations. As the Coast Guard and private contractors flew helicopters during the event to rescue citizens from flooded homes, media reports emerged that shots were being fired at those helicopters. Such reports were based on scanty (and in many cases, dubious) evidence. Nevertheless, Coast Guard and private sector rescue fights were halted in response.114

More troubling indications have since emerged that adversaries might intentionally spread disinformation via social media to incite public panic and disrupt response operations. On September 11, 2014, hundreds of

---


Twitter accounts began documenting a (non-existent) disaster at a chemical plant in St. Mary’s Parish, Louisiana. Supposed eyewitnesses provided false images of explosions, flames engulfing the plant, and thick black smoke pouring from the facility. Dozens of media outlets and public officials found their Twitter accounts inundated with such messages, including a realistic-appearing screenshot of CNN’s homepage intended to provide credibility by showing that the disaster had already made the national news. Subsequent press accounts identified Russian entities as being the source of this disinformation operation.115

**Finding**

*Combined attacks using cyber, kinetic, and information operations would magnify the challenges of sustaining and restoring critical infrastructure services in a catastrophic event.*

The GridEx exercise series has pioneered the use of scenarios that include both cyber and kinetic attacks and has highlighted the risk that such hybrid warfare operations would create especially wide area, long duration outages. These exercises have helped utilities build plans and coordinating mechanisms for power restoration in extreme events. Other infrastructure sectors could face combined cyber/kinetic threats as well and would benefit from creating equivalent exercises and planning initiatives. However, no exercises to date, in any sector, have addressed the risk that adversaries will use false reporting on social media to disrupt infrastructure restoration operations. Nor has the Federal government yet developed strategies or concepts of operation to combat such targeted disinformation campaigns, despite indications that the risks of information warfare are increasing.

*Recommendation: Infrastructure owners and operators should partner with their Sector-Specific Agencies to build preparedness against combined threats.*

---

New forms of government-industry collaboration will be required against coordinated cyber, kinetic, and information operations. For example, to prepare for the risk of actual (or even falsely reported) active shooter threats against forward-deployed infrastructure employees, new plans and concepts of operation will be required for expanded security support. National Guard forces in State Active Duty or Title 32 Status (both of which enable Guard personnel to perform law enforcement functions) offer a prime opportunity to supplement local and state law enforcement security support operations. However, very few states have such plans in place. Dialog between infrastructure leaders and their state law enforcement and National Guard counterparts will be essential to identify (and develop plans to address) potential security requirements, and carry out exercises to strengthen operational effectiveness in implementing those plans.

Fewer near-term options exist to counter the risks posed by information warfare. One starting point would to leverage Emergency Support Function (ESF) 15, External Affairs. ESF-15 is designed to help DHS and its partners provide “accurate, coordinated, timely, and accessible information to affected audiences, including governments, media, the private sector, and the local populace…”116 Many infrastructure sectors have also built communications playbooks with their respective SSAs to coordinate messaging on infrastructure restoration timelines. Building on these established playbooks and ESF-15, new organizational designs may offer an expeditious way forward to prepare for countering disinformation campaigns.

e. Strategic Implications for Building Cross-Sector Resilience

Manmade threats will entail cross-sector requirements above and beyond those necessary for natural hazards. For natural hazards, operations to sustain and restore critical services will need to focus on those systems essential for saving lives, and for maximizing the number of survivors who can shelter in place rather than evacuate. Water utilities, food distribution centers, major hospitals and the infrastructure functions on which they

---

depend (including electricity, communications, and transportation) will be prime candidates for prioritized, cross-sector support.

Keeping these facilities and functions up and running will also be vital against manmade threats. However, adversaries may also target U.S. critical infrastructure to intentionally disrupt and degrade U.S. national defense capabilities. Long duration, wide area outages would jeopardize American military bases’ ability to perform Mission Essential Functions (MEFs) and sustain mission assurance. The Department of Defense 2012 Mission Assurance Strategy cautions that “Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting critical Defense and supporting civilian capabilities and assets … on which our forces depend.”117 Indeed, “Threats to non-DoD government and commercially owned infrastructure, facilities, and capabilities … can jeopardize DoD mission execution,” in part due to DOD’s dependence on civilian infrastructure.118 Preparing to help sustain and (as needed) rapidly restore the infrastructure on which key Defense installations depend will be vital for national security.

DOD’s 2012 Mission Assurance Strategy cautions: “Potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting critical Defense and supporting civilian capabilities and assets … on which our forces depend.”

Finding

Manmade threats will require additional criteria for prioritizing infrastructure sustainment and restoration.

We should expect that adversaries will target the specific infrastructure systems that support key military bases and other national security

118 Ibid.
facilities. In particular, adversaries will likely seek to disrupt the ability of these bases to function by creating multi-state, cascading failures of critical infrastructure. Cross-sector resilience planning should account for these risks and prioritize support for national security facilities and functions accordingly.

**Recommendation:** *DHS and its partners should build a Black Sky Prioritization List (BSPL) to provide a comprehensive, all-hazards basis to target cross-sector infrastructure sustainment and restoration operations.*

The section that follows examines the criteria that should drive this prioritization process and analyzes how existing lists of critical infrastructure can be leveraged to build preparedness for Black Sky events.
The lack of adequate criteria to effectively prioritize infrastructure sustainment and restoration operations has been a long-standing challenge. The 2014 National Security Telecommunications Advisory Committee (NSTAC) report found that “there is currently no protocol for the Government to convey in advance the national cyber priorities for protection, reconstitution, or recovery in the event an incident surpasses industry’s

The U.S. government and its industry partners do not have a mechanism to prioritize sustainment and restoration operations across critical infrastructure sectors.
mitigation ability.” A 2016 Homeland Security Advisory Committee report found that these gaps have continued, and that “Significant improvements are needed in assessments of cross-sector vulnerabilities and in mechanisms to prioritize restoration operations accordingly.”

Nevertheless, a number of efforts are already underway to identify infrastructure that would be especially important to sustain and restore in catastrophic events. Taken together, these initiatives provide an enormously valuable foundation for building a Black Sky Prioritization List (BSPL).

1. **Section 9 List Methodologies**

   The methodologies developed to implement Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, provide the most comprehensive starting point for the Black Sky Prioritization List. Section 9 of this order instructs the Secretary of Homeland Security to “identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.” The list assembled to satisfy this Section 9 requirement was never intended to be used as an all-hazards prioritization scheme to guide cross-sector sustainment and restoration in Black Sky outages, and its inclusion in the EO aligns it to serve other objectives. Nevertheless, the methodologies behind the Section 9 list can provide a valuable starting point for identifying the most critical infrastructure assets in these scenarios.

   Using the Section 9 methodologies as the basis for Black Sky planning would require the further identification of key facilities for non-cyber incidents. The

---

increasing cyber connectivity of critical infrastructure networks and systems, however, narrows the gap between the Section 9 approach and one that would consider all hazards. Infrastructure owners and operators should be able to use the Section 9 data to supplement their existing plans to prioritize service sustainment and restoration, and support cross-sector coordination on a nationwide basis.

Major impediments exist to doing so, however. While the Department of Homeland Security (DHS) informs asset owners that they are on the Section 9 list, those owners are not told which similarly critical facilities in other sectors are nearby, hobbling efforts to improve cross-sector situational awareness and build prioritized sustainment and restoration plans.

Yet, securing and close-holding this classified data is vital; in the hands of adversaries, the Section 9 list or equivalent prioritization efforts would provide a strategic roadmap for attack, serving as an instructive guide on how to maximize the devastation of U.S. critical infrastructure. However, an improved scheme of providing the appropriate individuals with sufficient security clearance to enable planning and situational awareness may prove vital. Otherwise, the list’s utility may be limited in actual emergencies.

The Federal government will also face inherent problems in maintaining an updated list of the most critical infrastructure assets and components nationwide. Indeed, building a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Even more difficult will be ensuring that individual utilities provide the data necessary to update that list on an ongoing basis. In the U.S. food distribution industry, the liquid fuels network, and other sectors vital for Black Sky resilience, efforts to cut costs and increase efficiency are scouring away redundant infrastructure and constantly shifting the landscape of cross-sector vulnerabilities. As examined in Section II, however, even small changes to system configurations in one industry can produce unintended and unforeseen effects on overall system resilience. Yet, companies have powerful incentives to resist sharing such business-sensitive, proprietary information. DHS will therefore have to strengthen business leaders’ confidence that government agencies would not use this data for regulatory compliance, antitrust, or other purposes not explicitly approved by those leaders.
2. Other Prioritization Efforts

Government and industry leaders will need to supplement the Section 9 data to provide a more comprehensive understanding of critical infrastructure networks and sustainment and restoration priorities. Other prioritization schemes may be particularly helpful when integrated into a broader effort, but are unlikely to contend with the Section 9 methodologies as the basis for the BSPL due to specific deficiencies.

a. Cybersecurity Strategy and Implementation Plan (CISP) and High Value Assets (HVA)

One such effort comes from the Office of Management and Budget (OMB), which launched a Cybersecurity Strategy and Implementation Plan (CSIP) in October 2015. The CSIP’s main objectives include the prioritized identification and protection of high value assets and rapid recovery from incidents when they occur. The CSIP included a directive for all departments and agencies to “identify their high value assets (HVAs) and critical system architecture in order to understand the potential impact to those assets from a cyber incident and ensure robust physical and cybersecurity protections are in place.”

Supplemental guidance released in December 2016 defines HVAs as: “assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.” This definition closely mirrors that of EO 13636.

Unlike for DHS’ Section 9 list, however, OMB publicly provides guidance on how to identify such assets. Among this guidance, OMB states that: ‘Agencies’ assessment of risk should consider not just the risk that an HVA poses to the agency itself, but also the risk of interconnectivity and

123 Ibid.
interdependencies leading to significant adverse impact on the functions, operations, and mission of other agencies.” This cross-sector approach to identifying vulnerabilities among interdependent infrastructure is certainly valuable.

The CSIP and HVA list have one major flaw, however: they are not limited or specific to critical infrastructure, and therefore the categorization scheme may prioritize certain assets that are important but not essential to sustainment and restoration of lifeline infrastructure in a Black Sky outage. This broader set of priorities could risk delaying or otherwise impeding efforts that are required to avoid cascading failures and further catastrophe.

b. Infrastructure of Concern (IOC)

DHS also creates infrastructure of concern (IOC) lists in response to incidents or hazards that threaten critical infrastructure. IOC lists are created on an incident-specific basis with the intent to “inform the strategies of Federal, State, local, and private sector partners… [creating] a prioritized list of infrastructure for significant federal response activities.”

The dynamic nature of these lists may be especially useful in predictable events with a reasonably estimated impact area, such as hurricanes or other severe terrestrial weather. Experience using IOC lists could also generate valuable lessons learned about how response operations can be more agile and adapt to changing conditions in an outage. For Black Sky events, however, the IOC list will also be entirely inadequate. For unpredictable catastrophic outages, a prioritized list such as the BSPL must exist before disaster strikes to enable rapid and/or proactive support. Necessary long lead efforts to harden vital infrastructure components before a Black Sky event, too, cannot be based on an ad hoc list.

c. National Critical Infrastructure Prioritization Program (NCIPP)

The IOC lists are complemented (and in fact informed in part) by DHS’ National Critical Infrastructure Prioritization Program (NCIPP). The NCIPP identifies and prioritizes infrastructure which could cause catastrophic consequences if disrupted, creating tiered asset prioritization categories to inform DHS protection and risk mitigation efforts.\textsuperscript{127} The GAO, however, has criticized changes that DHS has made to the NCIPP to accommodate certain sectors, which constitute a departure from the National Infrastructure Protection Plan (NIPP) approach, and could “hinder DHS’ ability to compare infrastructure across sectors.”\textsuperscript{128} This cross-sector aspect of prioritization will perhaps particularly critical in Black Sky outages. The GAO report therefore highlights important issues that raise questions about the NCIPP’s potential value for contributing to the BSPL.

d. Threat and Hazard Identification and Risk Assessment (THIRA)

Within DHS, FEMA also has its own separate system to guide emergency operations planning. The Threat and Hazard Identification and Risk Assessment (THIRA) process is less suited to critical infrastructure sustainment and restoration, as it focuses on a whole community approach, including “individuals, businesses, faith-based organizations, nonprofit groups, schools and academia…”\textsuperscript{129} To be sure, it will be important for all community stakeholders to understand the risks involved in catastrophic outages, and how they may be affected. However, THIRA does not focus specifically on the critical infrastructure sustainment and


\textsuperscript{128} Ibid.

restoration requirements that will be essential to minimizing the negative impacts of catastrophic outages. A senior FEMA official from the Obama administration also noted that while the THIRA methodology could have some merit if properly applied, it has become “simply a means to identify risks in such a way as to access grant dollars.” As a result, THIRA lists are not likely to make a valuable contribution to building a comprehensive BSPL unless the methodology is applied more relevantly to the cyber-physical aspects of critical infrastructure.

e. National Essential Functions

Another approach is centered around National Essential Functions, defined in the U.S. National Continuity Policy (PPD-40). While PPD-40 itself is classified, limiting potential analysis in this volume, Executive Order 13744 regarding severe space weather provides some insight. Indeed, EO 13744 directs Sector-Specific Agencies to “ensure that space weather events are adequately addressed in their all-hazards preparedness planning, including mitigation, response, and recovery” to protect the National Essential Functions.130 This implies a prioritization scheme exists to define the National Essential Functions, and the critical infrastructure assets that are required to sustain them. These efforts, however, appear to be stovepiped for each SSA, limiting the list’s value for cross-sector infrastructure sustainment and restoration in a Black Sky outage.

f. Telecommunications Service Priority (TSP)

The communications sector has made some notable progress in industry-government prioritization efforts. The Federal Communications Commission (FCC) and DHS are working with industry under the Telecommunications Service Priority (TSP) program to prioritize vital service restoration to critical national security and emergency preparedness functions in crises. The TSP program mandates telecommunications utilities to restore service according to a defined list of priorities in an

attempt to “minimize service interruptions that may have a serious, adverse effect on the supported NS/EP functions.”

While the TSP is a good starting point, the program works on a voluntary enrollment basis. This makes it more difficult to ensure that all of the truly most important priorities have their service restored first. Indeed, failure to enroll in the program means that – no matter its importance – telecommunications service providers cannot restore service to an affected utility until they have restored all TSP priority lines. It is also not clear if TSP prioritizations are based on an understanding of the complex interdependencies and single points of failure that underlie critical infrastructure networks.

g. Utility Owner and Operator Lists

Utilities often have their own plans to prioritize restoration following disruptions or outages. These utility plans will offer vital contributions to building the BSPL. However, utility-led prioritization efforts tend to suffer from three particular shortfalls.

First, they are unlikely to employ the cross-sector approach necessary for sustainment and restoration in a long duration, wide area outage, including information sharing to identify key assets and restoration profiles from other sectors in their service areas.

Crews working to restore natural gas infrastructure (Source: FEMA)

Second, utilities may not be fully aware of all critical national security functions and facilities in their service footprints. Given the (appropriate) secrecy with which much of the data and information pertaining to national security are handled, some aspects of this process must be inherently governmental functions.

Third, many current priority lists assume less system impact than in Black Sky events will create. To plan for and implement the restoration of service to critical facilities and functions, utilities will need to account for the risk of massive damage to their systems, including the possible destruction of infrastructure essential for both primary and backup black start cranking paths.

One option to build such preparedness would be to pre-identify and extensively harden a protected “backbone” of grid infrastructure, scaled to survive Black Sky hazards and restore the loads that will be critical for public safety and national security in such events.\(^{133}\) As the Department of Energy designates Critical Electric Infrastructure (CEI) and Defense Critical Electric Infrastructure (DCEI) under the Federal Power Act (as amended), those designations could further support targeted hardening efforts and prioritized restoration planning.\(^{134}\) Equivalent resilience efforts should extend to all critical infrastructure sectors.

3. Building a Cross-Sector Focus for Prioritization

Sector response and recovery paths differ from one another considerably. Acting individually, each sector develops optimal response and recovery priorities that minimize the degree and duration of their respective service outages. Optimization should instead take a ‘system of systems’ approach to ensure that overall recovery takes place in the minimal amount of time.

\(^{133}\) On backbone approaches to grid restoration, see: FERC and NERC, Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans, January 2016, pp. 8, 55.

\(^{134}\) The Fixing America’s Transportation Act (2015) amendments to the Federal Power Act include definitions of CEI and DCEI for the purpose of identifying the infrastructure most critical to national security and defense, economic security, and public health and safety. See: Section (a), 16 U.S.C. § 824o–1, https://www.law.cornell.edu/uscode/text/16/824o-1.
The U.S. is collectively far from the required coordination and prioritization necessary for effective cross-sector sustainment and restoration in Black Sky-level events. However, the alternative to prioritization – disorganized competition – is not at all feasible and will cost lives.

Finding

Section 9 of Executive Order 13636 provides the best methodological starting point to identify sustainment and restoration priorities for Black Sky (and less severe) events.

While the Section 9 list was developed to strengthen resilience solely against cyber threats, the methodologies used to develop the list can and should be adapted to build preparedness against the full range of Black Sky hazards, and to account for emerging cross-sector interdependencies.

Recommendation: Government agencies and their industry partners should use the Section 9 methodologies as a foundation to build a Black Sky Prioritization List (BSPL).

The BSPL should leverage all available data to identify the very most critical facilities and functions to avert catastrophic damage to national security, the economy, and public health and safety in Black Sky events. Once the BSPL is established, Playbook developers can build plans to sustain (or rapidly restore) essential infrastructure services to those BSPL assets, and account for the cross-sector support that sustainment and restoration operations will require. The BSPL should also help guide investment to harden the infrastructure on which those critical facilities and functions depend.
Finding

Identifying critical facilities (especially in the context of cross-sector interdependencies and operations) presents significant challenges.

EO 13636’s Section 9 requirements create a “corporate” level list that is not broken down to the key priorities within the corporation (i.e., facilities, systems, and nodes). Moving to a more fine-grained level of analysis will be essential to support Black Sky planning. However, at that deeper level of analysis, the increasingly complex, multi-layered, and interdependent nature of U.S. infrastructure will present additional challenges in identifying key assets and the consequential relationships between them.

Recommendation: Leverage GINOM modeling and simulation to identify critical facilities.

EIS Council is developing GINOM specifically to address these complex and critical modeling challenges. In partnership with industry and government, GINOM project sector leaders should use the tool’s simulations to pinpoint key facilities and functions for inclusion on the BSPL, and (through interdependency analysis) identify “hidden” criticalities. DHS-sponsored programs, including the RRAP initiative, should also be leveraged to support this effort.\textsuperscript{135}

IV | INFRASTRUCTURE OWNERS AND OPERATORS: CROSS-SECTOR PLANNING AND COORDINATION FOR BLACK SKY RESILIENCE

Black Sky events will require infrastructure owners and operators to collaborate in extensive cross-sector sustainment and restoration operations, and do so when normal communications systems will be unavailable or severely disrupted. This cross-sector coordination should begin long before Black Sky hazards strike, allowing utilities in all sectors to collectively pre-plan for mutual support.

A number of initiatives to strengthen cross-sector collaboration are already underway. Most important, the coordinating councils of the electric subsector, the financial services sector, and the communications sector have established a Strategic Infrastructure Coordinating Council (SICC) to develop and exercise
cross-sector response plans and interface with government leaders.\textsuperscript{136}

The establishment of the SICC constitutes an extraordinary step forward. However, to meet the challenges of Black Sky events, industry leaders will need to expand the SICC’s approach over time to include additional sectors and capabilities for operational coordination. The section that follows examines opportunities to do so. In particular, this section proposes the creation of a Cross-Sector Coordinating Council (CSCC) that would leverage the progress being made under the SICC.

The proposed CSCC would build on the SICC in four ways. Specifically, the CSCC will:

1. **Expand to Include All Sectors.** CSCC membership should include all critical infrastructure sectors and key supply chains, and evolve to provide connectivity with international resource suppliers.

2. **Advance Planning and Real-Time Coordination.** As a key function, the CSCC should plan and prepare mechanisms to carry out the specialized, real-time coordination functions that will be of the greatest importance to Black Sky response operations (including those related to emergency communications and power).

3. **Coordinate with Regulatory Agencies.** The CSCC can serve as a locus for industry leaders to collaborate with regulatory bodies in all sectors to facilitate coordinated Black Sky protection planning and implementation.

4. **Ensure Effective Implementation.** The CSCC should also help ensure that the decisions made by the Council’s industry representatives will be implemented on an expanded, multi-sector basis.

1. Building on Progress to Date

In the face of intensifying challenges posed by cascading failures, coordination among all 16 critical infrastructure sectors will be essential for avoiding unplanned mass migration and supporting national security. This section examines the initial step to provide for comprehensive industry coordination: the creation of mechanisms that will enable infrastructure owners and operators to assist each other on a prioritized, multi-sector basis. Once established, similar coordination will be needed between this group of sector leaders and government agencies (and ultimately, NGOs).

Owners and operators have unique knowledge of their systems, capabilities, and support requirements. They will also play a key role in approving and implementing the delivery of assistance in Black Sky events. Industry must therefore play a leading role in cross-sector resilience planning and operations.

Until recently, however, progress towards establishing cross-sector coordinating mechanisms has been slow. One reason is that infrastructure sectors are structured in different ways. They vary in terms of whether they prefer CEOs to represent their sectors, as opposed to less senior leadership. They differ in the degree to which representatives can commit resources for their entire sectors, as opposed to only their own companies. Their approaches to emergency coordination reflect disparate regulatory, antitrust, and intra-sector competitive environments. They also vary in the number, size, and diversity of organizations within them, ranging from a handful of globally-oriented companies in the communications sector, to over 160,000 independent water and wastewater systems in the water sector.

The slow pace of establishing cross-sector coordination mechanisms also reflects the novelty of the effort. Until recently, sector coordinating councils focused almost exclusively on their sector-specific issues. And while DHS is responsible for Federal coordination across the full range of infrastructure sectors (supported by SSAs), eliciting Federal support for an industry cross-sector council to interface with the government requires significant policy and organizational change – never an easy thing to accomplish.
The evolution of the Strategic Infrastructure Coordinating Council exemplifies these challenges. In 2015, the National Infrastructure Advisory Council (NIAC) recommended that the Secretary of Homeland Security work with the Sector-Specific Agency heads of the electric, water, transportation, communications, and financial services sectors to establish a Strategic Infrastructure Executive Council (SIEC). The SIEC was to be composed of CEOs or other senior executives from these sectors and agencies who would “identify national priorities and develop joint or coordinated action plans and agreements to implement them.”\(^{137}\) However, despite extensive discussions between DHS and industry representatives in 2015 and 2016 on this recommendation, the SIEC was never established.

Instead, the creation of a Strategic Infrastructure Coordinating Council (SICC) is now moving forward. With support from the NIAC, the coordinating councils of the electric subsector, the financial services sector, and the communications sector have established the SICC to advance goals that are critical for disaster preparedness. In particular, in support of these three sectors, the SICC will:

\[\text{...identify mutual priorities, develop and exercise cross-sector incident response plans and protocols, as well as align organizations, systems, processes, and technologies across sectors. The SICC also will serve as a focal point for government engagement with strategic infrastructure in steady state and during crises.}\(^{138}\)

Ongoing efforts by the electric subsector and other sectors to create Black Sky Playbooks can help the SICC jump-start its cross-sector planning efforts. However, building preparedness for Black Sky events will require the inclusion of a broader range of infrastructure sectors than those currently included in the SICC. Eventually, this should also extend to key resource and service sectors, and selected segments of their supply chains – most of which will require significant international coordination. Such catastrophic events will also require

---


industry leaders to coordinate sustainment and restoration operations in the face of unprecedented cross-sector failures, including major communications outages. Leveraging the SICC to create a Cross-Sector Coordination Council (CSCC) could help address these gaps.

Finding

One size will not fit all in terms of sector participation.

Given the wide variation in the way sectors are structured, and the voluntary nature of cross-sector coordination, individual sectors will need leeway to determine how they should be represented in the CSCC.

Recommendation: The CSCC should allow sectors to determine how they will be represented in the Council.

Sector-specific variability in representation should include how those representatives can help guide the sector’s contributions to cross-sector sustainment and restoration operations. This is especially important for sectors with a large number of individual owners and operators.

Finding

The CSCC should determine the best way to coordinate with government agencies.

One of the most valuable goals of the SICC is to provide for an integrated, cross-sector focal point for engaging with government during crises. This key attribute will be essential for an effective CSCC structure.

Recommendation: Industry leaders should review lessons learned to formulate CSCC-government coordination structures.

To develop the Cross-Sector Coordinating Council, industry leaders should examine lessons learned from past disasters to propose how government engagement should be structured. For example, during Superstorm Sandy (2012), the Federal Emergency Management Agency (FEMA) and the ESCC cobbled together an Energy Restoration Task Force to facilitate government-industry collaboration for power restoration. However, such ad hoc collaboration will be woefully inadequate in a Black Sky outage.
As will be discussed in the section that follows, the Federal government has not yet planned or organized for operational coordination with multiple infrastructure sectors. Infrastructure owners and operators should determine how best to structure the interface between their cross-sector coordination council and government partners, consistent with the National Response Framework and other key sources of guidance on disaster response.

An equivalent effort will be necessary to structure the interface between the CSCC and state, local, tribal, and territorial (SLTT) government officials. The National Emergency Management Association recently found that these officials lack the unified guidance they require to structure their partnerships with infrastructure owners and operators and other private sector leaders.\textsuperscript{139} The CSCC should also determine how best to interface with SLTT officials, and account for the vast number of them that will want to be engaged on response issues in multi-region Black Sky events.

**Finding**

*Emergency communications will be a key enabler.*

The CSCC will be useless if its members are unable to communicate in a Black Sky event. A growing number of infrastructure companies are upgrading their backup communications systems to help sustain their own functions if primary systems are disrupted. However, to guide cross-sector support operations, survivable and secure emergency communications links will also be needed between sector leaders and: system operators within their sector; system operators in partner sectors; government agencies; mass care NGOs; and a wide array of private and public sector resource providers. Current capabilities for cross-sector emergency communications (voice and data) require drastic improvement.

**Recommendation:** *Industry and government leaders should examine the Black Sky Emergency Communications and Coordination System (BSX\textsuperscript{TM}) as a Black Sky-compatible communication platform option.*

Chapter II of this volume examines the BSX™ system, which is designed to serve as a widely-distributed, interoperable, Black Sky hazard-protected emergency communication system that can survive for extended periods without grid-provided power.

Finding

Exercises will be essential to successful cross-sector coordination.

One of the keys to the effectiveness of mutual assistance in the electricity subsector is that CEOs and their staffs not only use their coordination mechanisms in hurricanes and other “real world” events, but also exercise the use of those mechanisms against more severe catastrophes than the United States has yet to experience. These exercises help the subsector identify and later mitigate gaps in planning and coordination, and validate successful initiatives. The CSCC should take a similar approach, building a foundation for multi-sector collaboration and improving its effectiveness long before Black Sky hazards strike.

Recommendation: The CSCC should participate in cross-sector exercises and less severe emergency response operations to prepare for Black Sky outages.

Once established, the CSCC should be used as frequently as possible to support cross-sector operations in real world events, even if those disasters are relatively small in scale. Doing so will help build cross-sector trust and operational expertise that will be critical in more catastrophic events. To strengthen Black Sky preparedness, the participation of CSCC members and staff in the EARTH EX exercise system would be enormously valuable for testing the viability of specific cross-sector coordination options and models.

Finding

Situational awareness will be critical to CSCC operations.

For the CSCC to effectively prioritize and coordinate cross-sector infrastructure operations in a Black Sky event, Council members will need to be able to establish situational awareness over the extent of disruptions in multiple interdependent sectors.
Recommendation: Foster the development of comprehensive, multi-sector situational awareness (SA) capabilities.

Recent events such as Hurricanes Harvey, Irma, and Maria have displayed significant progress in cross-sector information sharing and overall resilience. DOE provided detailed daily updates on restoration in both the electric and ONG subsectors, and the ESCC provided information on joint efforts with USACE. The FS-ISAC relayed information about the status of ATMs and merchants, including medical, hardware, department, and grocery stores to FEMA, the NICC and cross-sector partners. FEMA also provided frequent updates on “coordinated Federal support” efforts in Puerto Rico and the U.S. Virgin Islands. FEMA’s National Business Emergency Operations Center (NBEOC) provided members with access to an online operations dashboard. The government of Puerto Rico also aggregated detailed updates on restoration progress in its own multi-sector situational awareness dashboard, available to the public.

All of these improvements in SA should be leveraged to help plan and execute sustainment and restoration operations in Black Sky events. However, such events will require vastly more data on infrastructure, resources, critical services, and supply chains. Such data will also need to be communicated and used for decision support in a much more extensively degraded environment. In addition to leveraging these SA improvements, the CSCC will need to foster the development of new approaches to collect, expand, and provide such data for hosting by emergency communication systems like BSX, and for processing by comprehensive simulation models for decision support. The BSX system described in Chapter II, configured to support the GINOM multi-sector simulation model, is designed to help fill these gaps.

---


Figure A provides a notional diagram of how the CSCC would be structured.

2. Requirements for Successful CSCC Operations

The CSCC needs to meet a number of critical requirements to ensure it can fulfill its envisioned role and functions in Black Sky events. To do so, the CSCC must address four major needs:

a. Include representation and active participation from all critical infrastructure sectors and key supply chains.

Most efforts to increase resilience against Black Sky hazards are occurring in sector silos. Even the most advanced initiative to date, the SICC, currently involves only the electric, communications, and financial services sectors.\(^{142}\) There are other promising partnerships and initiatives involving multiple sectors. However, they are often limited to two or three sectors, based on specific shared issues or challenges. Given the widespread devastation that Black Sky events will inflict, all critical infrastructure sectors must jointly plan and prepare for such events and ensure the availability of resources to support each other.

b. **Enable specific operational functions that will be crucial in Black Sky events.**

In the response to Hurricane Maria in Puerto Rico, infrastructure leaders and their government partners made progress in conducting cross-sector operations. However, industry will need to both deepen and expand that operational coordination for Black Sky events. To do so, the CSCC will need to meet additional support requirements. Coordinating and prioritizing emergency power resources will be particularly critical. Ensuring resilient supply chains to deliver vital resources, including chemicals for water treatment, will pose additional requirements.\(^{143}\) The CSCC can bolster industry’s ability to meet these challenges by facilitating extensive pre-planning and capability development.

c. **Work proactively with government regulators in all sectors, at multiple jurisdictional levels.**

In Black Sky events, the infrastructure owners and operators leading sustainment and restoration operations will need to make quick decisions in what will likely be life or death situations. Failure to act could be extremely costly, and the middle of a Black Sky event is not the time to be negotiating detailed waivers and/or cost recovery mechanisms. Moreover, to prepare for such catastrophes, decision makers will need to build-in and

---

likely test new resilience capabilities that will enable essential sustainment and restoration operations in wide area, long duration outages.

CSCC leadership should work closely with local, state and Federal regulatory bodies to ensure that regulations which are essential in everyday operations will not be prohibitive in major catastrophes. Essential preparatory resilience-building and testing efforts before the onset of a Black Sky event may also trigger the need for waivers and cost recovery by utilities and corporations, which the CSCC can help facilitate.

d. **Establish and formalize decision-making authority.**

Industry representatives in the CSCC will need to ensure that the decisions they make are implemented. Meeting this requirement will pose a significant challenge, given the disparate ways in which infrastructure sectors are organized, and the degree to which precedents exist for providing guidance to their component utilities and companies. In some sectors, antitrust issues may also need to be addressed to facilitate effective collaboration in Black Sky planning and operations.
Sustaining and restoring critical services in Black Sky events will require a fundamental repurposing of the U.S. incident response system. That system is focused on delivering Federal assistance to states and localities when their own resources prove inadequate. However, in Black Sky events, industry – supported by the broadest possible coordination with the government and NGO sectors – must lead efforts to sustain and rapidly restore critical infrastructure services to save lives and protect U.S. security.

The current system is poorly structured to facilitate industry-led operations. U.S. policies and organizational diagrams create the appearance that the response system is structured to incorporate such operations. Yet, beneath the surface, major gaps exist in the readiness of government agencies to do
so, especially for the cross-sector infrastructure sustainment and restoration operations that will be so crucial in Black Sky events.

Filling these gaps by building a new, separate response system only for Black Sky events would be unwise and politically impractical. The National Response Framework and the coordination mechanisms that it supports are so deeply embedded in the United States, and so closely aligned with the Federal system of government and key acts of Congress, that developing and maintaining a “just break glass” system solely for Black Sky events would be extraordinarily difficult.

Doing so is also unnecessary. The existing U.S. response system has all the key components needed to build preparedness against Black Sky hazards. The analysis that follows examines how industry and government can partner to supplement this system for Black Sky events and realign it to put industry-led operations at the heart of emergency management. Three such efforts will be especially important:

- **Cross-Federal integration.** In the aftermath of Superstorm Sandy, a growing number of Sector-Specific Agencies (SSAs) have been improving their ability to coordinate incident response efforts with their respective infrastructure sectors. However, for cross-sector operations, much stronger unity of effort will be needed across the Federal government to help prioritize and support industry-led efforts, and provide a counterpart to the proposed Cross-Sector Coordinating Council (CSCC). This section proposes how the Federal Emergency Management Agency (FEMA) can collaborate with SSAs to meet cross-sector requirements. The section also assesses shortfalls in current Federal guidance on goals and priorities for infrastructure operations, and examines options to supplement the National Response Framework (NRF) and other key documents to fill these gaps.

- **Federal-state coordination.** Governors are responsible for public health and safety in their states. Accordingly, they will play a key role in providing emergency response assistance and helping industry prioritize response operations. To support governors in those roles, a
growing number of their state emergency operations centers (EOCs) are incorporating representatives from the private sector, especially from electric utilities. That representation is extremely valuable; consideration should be given to expanding it to include a broader range of critical infrastructure sectors.

However, Black Sky events will damage and destroy infrastructure across major portions of the United States and create immense challenges for prioritizing sustainment and restoration operations between states. FEMA and the U.S. President will need to bolster their ability to provide political “top cover” for infrastructure owners and operators in this unprecedented environment and strengthen unity of messaging as competing interstate priorities come to the fore.

- **Revamping the Emergency Support Function (ESF) system for cross-sector infrastructure operations.** ESFs provide the primary Federal coordinating structures for building, sustaining and delivering key functionally-oriented assistance capabilities. There are 14 ESFs, each having a Federal Department or Agency coordinator (see Annex A). Many states also rely on the ESF system to serve the same fundamental goals. However, the ESF system is focused on delivering government capabilities; many ESFs provide for only limited industry participation. Moreover, ESFs are heavily stovepiped. This chapter proposes options to remedy these shortfalls, including significant private sector participation and the creation of a new ESF dedicated to building, sustaining and delivering the capability that will be most needed in Black Sky events: Cross-Sector Coordination (ESF-14).

---

A. Integrating the Federal Government Into Cross-Sector Infrastructure Support Operations

While infrastructure owners and operators will play the most important role in helping each other sustain and restore critical services, government support for those efforts will be essential to help them succeed.

Earlier sections of this chapter have already examined key Federal support roles. They include:

- Pre-event responsibilities, such as partnering with industry to develop and continuously refine a Black Sky Prioritization List, and improving Federal Agency plans and capabilities to perform traditional assistance missions.
- Coordinating with states, local governments, and industry to incentivize and enable sustained operations for food, fuel, and other key resource providers in Black Sky scenarios.
- Encouraging and supporting multi-sector communication and coordination tooling.
- Post-event response functions such as providing security for response and recovery operations, and helping industry meet the emerging threats posed by information warfare and active shooters.

The Federal government will also need the ability to closely coordinate with the proposed Cross-Sector Coordinating Council (CSCC). When Black Sky hazards strike, they are bound to create unexpected challenges, in addition to those which Black Sky Playbooks have anticipated. Across the Federal government, agencies will need the ability to partner with infrastructure owners and operators to adjust response priorities accordingly. Close industry-government collaboration will also be required to monitor the execution of infrastructure operations, and to help emergency managers focus on sustaining lives where – due to engineering constraints or prioritization criteria – restoration of services will be slowest.

The Energy Restoration Task Force created in Superstorm Sandy provides the largest-scale example of such “real world” collaboration at the Federal
level. Lessons learned from the Task Force continue to drive improvements in government preparedness to incorporate infrastructure restoration in emergency response efforts – especially the need to prepare in advance for coordinated decision-making, rather than (as in Sandy) build such mechanisms from scratch in the midst of the event.

However, the Energy Restoration Task Force focused on a single sector. Black Sky events will create cascading failures across all of society’s interdependent infrastructure, resource, and service sectors and put a premium on cross-sector coordination during restoration operations. The proposed CSCC will provide for such coordination on the industry side. To create an effective counterpart to the CSCC, the Federal government will need to go beyond its existing policies, plans, and organizational arrangements for integrating industry leadership into response operations. Agency leaders must be able to quickly transition from a policy-making focus to an operational role, coordinating vital actions in a highly-fluid operational environment.


The Trump Administration is only beginning to put its stamp on the U.S. incident response system. However, President Trump inherited a set of policies from previous administrations that will provide a strong foundation on which to build, as well as gaps for the administration to fill.

One such foundational inheritance is the “whole community” approach to incident management. In catastrophic events, government capabilities alone will not be sufficient to meet the needs of survivors, especially in the
immediate aftermath of an event (when government assistance will not yet be available). Instead, all components of society – including non-governmental organizations involved in mass care, operators of lifeline utilities, and their partner sectors – will need to help save and sustain lives. Craig Fugate, former FEMA Administrator, noted that:

*Government can and will continue to serve disaster survivors. However, we fully recognize that a government-centric approach to disaster management will not be enough to meet the challenges posed by a catastrophic incident. That is why we must fully engage our entire societal capacity.*\(^{145}\)

Infrastructure owners and operators, along with resource and service suppliers, will be key providers of that capacity. They will be essential both to help meet the immediate human needs of event survivors, and for supporting disaster response operations with communications, power, transportation, and other essential services that governments are unable to adequately provide. Moreover, whole community strategies recognize the need to account for cross-sector interdependencies. As former Administrator Fugate stated: “We cannot separate out and segment one sector in isolation; the interdependencies are too great…. We want the private sector to be part of the team and we want to be in the situation where we work as a team and not compete with each other.”\(^{146}\)

Fundamental policy requirements also exist for the U.S. response system to include private and public sector infrastructure leaders. Homeland Security Policy Directive (HSPD) 5, Management of Domestic Incidents (February 28, 2003), requires the Secretary of Homeland Security to “coordinate with the private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities and to promote partnerships to address incident management capabilities.”\(^{147}\)


\(^{146}\) Ibid., at p. 11.

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection* (December 17, 2003), takes requirements for public-private partnerships still further. HSPD-7 emphasizes that critical infrastructure and key resources provide the essential services that underpin American society. The Directive also notes that the majority of that infrastructure is owned and operated by the private sector. Accordingly, the Directive lays out three key sets of Federal responsibilities for engaging with infrastructure owners and operators:

- The Secretary of Homeland Security serves as “the principal Federal official to lead, integrate, and coordinate implementation of [critical infrastructure protection] efforts;”

- Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, the Directive designates Sector-Specific Agencies (SSAs) and requires them to “collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;” and

- DHS and the SSAs are explicitly directed to “collaborate with the private sector and continue to support sector-coordinating mechanisms to identify, prioritize, and coordinate the protection of critical infrastructure and key resources,” as well as share information related to those efforts.\(^{148}\)

Taken together, these statements of U.S. response goals and doctrine provide a strong basis for integrating infrastructure owners and operators into Federal decision-making, and for coordinating sustainment and restoration efforts in Black Sky events. But statements of policy alone cannot ensure preparedness for such collaboration. Applying those statements to the

---

operational frameworks that guide Federal decision-making, and to prioritizing response efforts in Black Sky events, will constitute a major challenge for the Federal government and its infrastructure partners.


   To transform U.S. strategies and policies into action when Black Sky events occur, two documents will be especially important in guiding Federal collaboration with infrastructure owners and operators: the National Incident Management System (NIMS) and the National Response Framework (NRF). NIMS provides the template for incident management; the NRF provides the structure and mechanisms for national-level incident management policy.149

   Infrastructure owners and operators and their corporate colleagues are integral to NIMS. The description of the System notes that “The private sector plays a vital role in emergency management and incident response and should be incorporated into all aspects of NIMS. Utilities, industries, corporations, businesses, and professional and trade associations typically are involved in critical aspects of emergency response and incident management,” and need to be integrated into the System’s management structures accordingly when incidents strike.150 This integration is being facilitated, for example, by electric utilities and other infrastructure sectors’ nationwide efforts to provide NIMS training for their emergency management personnel.151

   The National Response Framework is equally committed to incorporating private and public sector infrastructure leaders into the response system. The NRF notes that:

   > ...some businesses play an essential role in protecting critical infrastructure systems and implementing plans for the rapid reestablishment of normal commercial activities and critical

---


150 Ibid., at pp. 11-12.

infrastructure operations following a disruption. In many cases, private sector organizations have immediate access to commodities and services that can support incident response, making them key potential contributors of resources [required for national response].

The recent hurricane in Puerto Rico provides a number of prime examples, with Google’s parent company Alphabet committing to provide cell phone reception via the solar-powered balloons from their Project Loon program, Tesla sending hundreds of large-scale, solar-powered batteries and staff to install them, and German energy firm Sonnen GmbH providing microgrids to power at least 15 relief centers.153

However, support from a vastly greater range of businesses – of which many will also be subject to the catastrophic disruption that their efforts will be necessary to help mitigate – will be essential in Black Sky events. While, as the NRF notes, some private sector actors will play crucial roles in response efforts, major catastrophes will require an ‘all hands on deck’ type mobilization from all sectors. Those utilities and businesses that already play an essential role will be even more vital in Black Sky events – perhaps more so than the NRF has imagined.

The NRF also sets the strategy and doctrine for how the whole community builds, sustains, and delivers “response core capabilities” necessary for response operations. These capabilities, which are identified in the National Preparedness Goal, include critical transportation, mass care, and other functions that will be vital in Black Sky events.154

152 Department of Homeland Security, National Response Framework: Third Edition, June 2016, p. 11. The response mission includes 14 core capabilities: planning, public information and warning, operational coordination, critical transportation, environmental response/health and safety, fatality management services, infrastructure systems, mass care services, mass search and rescue operations, on-scene security and protection, operational communications, public and private services and resources, public health and medical services, and situational assessment. NRF, p. i.


The NRF singles out “infrastructure systems” as one of these core capabilities. The Framework describes this function as the ability to “Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.” The NRF lists four critical tasks required for this capability:

- “Decrease and stabilize immediate infrastructure threats to the affected population, to include survivors in the heavily-damaged zone, nearby communities that may be affected by cascading effects, and mass care support facilities and evacuation processing centers with a focus on life sustainment and congregate care services.
- Re-establish critical infrastructure within the affected areas to support ongoing emergency response operations, life sustainment, community functionality, and a transition to recovery.
- Provide for the clearance, removal, and disposal of debris.
- Formalize partnerships with governmental and private sector cyber incident or emergency response teams to accept, triage, and collaboratively respond to cascading impacts in an efficient manner.”

b. Building on the NRF: Specific Goals and Priorities for Black Sky Operations

The basic response goals established by the NRF provide the Federal government and its infrastructure partners with a solid foundation for progress. Most important, in defining the infrastructure core capability, the Framework emphasizes the need for both sustainment (“decrease and stabilize immediate infrastructure threats”) and restoration operations. Calling for formalized government-industry partnerships, the NRF provides a strong foundation for building Black Sky preparedness.

---

partnerships to “triage and collaboratively respond” to cascading failures also provides an important impetus for building Black Sky preparedness. Those partnership initiatives should be structured to go beyond the NRF’s statement of objectives and clarify the principles that will guide the triage and prioritization of infrastructure operations.

Despite the solid foundation of policy guidance and directives for Federal emergency response efforts, significant gaps remain between current capabilities and those required to effectively carry out cross-sector response operations in Black Sky scenarios. The following findings and recommendations aim to address some of these gaps.

**Finding**

_The NRF’s goals do not fully account for response priorities against manmade threats._

While the Framework is structured to guide response operations against all hazards, including adversary attacks, the document focuses on response efforts needed to “save lives, protect property and the environment, stabilize communities, and meet basic human needs following an incident.” These goals will be vital when adversaries strike U.S. critical infrastructure. However, to deter (and if necessary, effectively respond to) such attacks, the United States must also have the ability to sustain infrastructure services to major Defense installations and other national security-related facilities. In addition to the NRF’s existing societal focus and suggested Defense-oriented goals, preventing adversaries from inflicting catastrophic, long-term damage to the U.S. economy will be a crucial objective as well.

**Recommendation:** _DHS should supplement U.S. response frameworks to explicitly identify national security and economic survival as goals for government-industry collaboration._

If and when the Trump Administration updates the NRF, incorporating these additional objectives will help ensure their inclusion in follow-up

---

157 Ibid., at p. 1.
partnership initiatives for planning, exercising, and organizing for infrastructure sustainment and restoration operations. The NRF’s specific goals for the infrastructure core capabilities\textsuperscript{158} should be expanded accordingly.

A near-term opportunity also exists to formally adopt these goals. The NRF’s Catastrophic Incident Annex has not been updated since November 2008 and is in great need of revision. The Annex notes that in catastrophic events, the Federal government may establish a command structure to “protect national security” as well as achieve more traditional U.S. response objectives.\textsuperscript{159} The Annex notes that U.S. response efforts may also seek to “maintain the operation of critical infrastructure/key resources,” and calls for the inclusion of the private sector in planning for the Annex’s implementation.\textsuperscript{160} FEMA should revise the Catastrophic Incident Annex to feature national security and economic survival as key goals for such plans.

The FAST Act also provides a potential model to account for national security priorities within the U.S. response framework. The Act requires the Secretary of Energy, in consultation with relevant Federal agencies and utility owners and operators, to identify and designate facilities that are “(1) critical to the defense of the United States; and (2) vulnerable to a disruption of the supply of electric energy provided to such facility by an external provider.”\textsuperscript{161} DHS and other Federal stakeholders, in partnership with industry leaders, should establish a similar designation and subsequent list – perhaps leveraging the FAST Act-mandated list of critical defense facilities. This list should be factored into cross-sector prioritization initiatives that will inform sustainment and restoration operations.

\begin{itemize}
  \item \textsuperscript{158} FEMA identifies 32 core capabilities to “address the greatest risks to the nation,” as part of the National Preparedness Goal – 15 of which are relevant to the response mission area and therefore included in the NRF. See “National Preparedness Goal,” Federal Emergency Management Agency, last updated July 5, 2016, https://www.fema.gov/national-preparedness-goal.
  \item \textsuperscript{159} Department of Homeland Security, Catastrophic Incident Annex of the National Response Framework, November 2008, p. CAT-1.
  \item \textsuperscript{160} Ibid., at p. CAT-2.
\end{itemize}
Finding

The Federal government and its partners need additional criteria to prioritize sustainment and restoration operations.

The NRF and its annexes lack adequate criteria to prioritize sustainment and restoration operations in Black Sky events.

Catastrophic earthquakes and other multi-region Black Sky hazards will create a massive gap between requirements to sustain and restore critical services and the capacity of infrastructure owners and operators (and their government partners) to meet these needs. Prioritizing infrastructure operations in such events will be essential. While the NRF calls on government and industry leaders to be prepared to “triage” response efforts, the Framework does not provide sufficiently detailed criteria for doing so.

As suggested in Section III, government officials should partner with industry to develop and continuously refine a Black Sky Prioritization List. However, as infrastructure owners and operators and agency leaders focus on sustaining and restoring service to those assets, measures to meet many other community assistance requirements will be delayed. Industry and government officials should build consensus on how to manage those delays and allocate scarce response resources accordingly.

The most detailed Federal guidance for prioritizing infrastructure response operations is provided by the Critical Infrastructure and Key Resources (CIKR) Annex to the NRF. The Annex emphasizes the need for the Federal government to work with CIKR “owners and operators to clearly establish priorities for
prevention, protection and recovery” of such assets.\textsuperscript{162} To meet these needs, the CIKR Annex requirements for DHS include the following roles:

Identifying, prioritizing, and coordinating Federal action in support of the protection of nationally critical assets, systems, and networks, with a particular focus on CIKR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a weapon of mass destruction.\textsuperscript{163}

That tasking to DHS is useful but also inadequate as a guide for response operations. While the Black Sky Prioritization List will help DHS identify specific infrastructure assets for support, neither the NRF nor the CIKR Annex provide broader criteria to guide the allocation of scarce response resources in wide-area catastrophes. A senior Federal official has noted, however, that DHS and FEMA are partnering to re-do the CIKR with the goal of better incorporating the relationship between Federal partners into incident response and recovery.

Past disasters have highlighted the difficulty of making such decisions. In Superstorm Sandy, for example, officials needed to determine which tunnels and subway systems should be pumped out first, given the shortage of high-capacity pumps relative to need. Disputes over how to establish those priorities were intense. New York City and New York State officials gave conflicting guidance to the U.S. Army Corps of Engineers (USACE) on ranking tunnels for pumping and lobbied senior Defense officials to make their preferences stick.\textsuperscript{164}

Similar conflicts are bound to emerge across multiple infrastructure sectors in Black Sky events, when far greater threats will exist to public safety and national security.

To limit such disagreements and help response leaders resolve them, it would be enormously helpful if the NRF and its annexes could provide additional criteria to guide the allocation of decision-making authorities and scarce assets for sustainment and restoration.


\textsuperscript{164} Federal Emergency Management Agency, Hurricane Sandy FEMA After-Action Report, July 1, 2013, p. 28; Paul Stockton, Assistant Secretary of Defense during Superstorm Sandy, personal records from the event.
Recommendation: As FEMA regions build their own preparedness plans based on the POIA framework, they should build consensus on overarching principles to prioritize response operations and incorporate them in the NRF.

The POIA proposes broad guidelines for prioritizing response efforts in catastrophic blackouts. The Black Sky Playbook development process and other EIS Council efforts have also begun to identify options for allocating scarce response resources.

In particular, the EPRO Handbook II volume on the water sector advanced an industry-generated recommendation that – in addition to serving BSPL assets – sustainment and restoration efforts in a Black Sky event should aim to enable the largest possible number of people to shelter in place for the duration of the emergency. Avoiding the “tipping point” where sheltering in place is no longer feasible will ideally help avoid unplanned mass migration, which – as examined earlier in this chapter – will itself be catastrophic. Federal emergency planners and managers must consider this requirement when updating the NRF and the principles that guide response efforts in Black Sky events.

The emergency management community and its partners should develop options to supplement the NRF and its annexes with equivalent guidance, and provide emergency managers and their industry partners with the basic criteria that should be applied (and tailored as needed for specific local circumstances) to prioritize sustainment and response operations.

Finding

Informing the public about prioritization criteria will be vital.

Recent exercises, including the Liberty Eclipse Energy Cyber Incident Exercise (December 2016), have highlighted the problems that catastrophic events will create for communicating with the public on restoration of power, liquid fuel deliveries, and other critical services. A key finding from that exercise:

The public will face a great deal of uncertainty following a significant cyber incident that causes physical damage (such as a long-term power outage or petroleum disruption), creating a considerable challenge for public information
and expectation management, particularly around restoration times.\textsuperscript{165}

The AAR recommended that public information programs be included in emergency response planning. However, the Report does not address the question of what these programs should comprise, and how they can deal with public concerns that restoration of their own services might be delayed in deference to higher response priorities. The Critical Infrastructure and Key Resources Annex and the NRF Public Affairs Support Annex both call for the Federal government to coordinate with Sector-Specific Agencies to share information with the public on restoration operations.\textsuperscript{166} Yet, they also fail to offer guidance on how to address the politically-charged issues that prioritization will raise.

Recent hurricanes have demonstrated progress in public communication. Strong public-private coordination through the ESCC has supported restoration efforts and facilitated communication about restoration timelines.\textsuperscript{167} DOE provided daily updates and situation reports (though lacking specific information about timelines),\textsuperscript{168} and DHS is attempting to curb misinformation by vetting pervasive rumors.\textsuperscript{169} However, Hurricane Maria knocked out nearly all internet and cellular service in Puerto Rico,\textsuperscript{170} limiting the value of improved public communications to those affected by the catastrophic event. Black


Sky scenarios in the continental U.S., which will be even more severe due to their geographic extent, are likely to have a similar (or worse) impact on ICT. Moreover, public uncertainty and unrest will be significantly greater in such events, where fewer resources will be available to address a more challenging response effort, over a longer period of time.

Recommendation: **Government authorities at the local, state and Federal level should share prioritization criteria more broadly to support whole community preparedness.**

In Black Sky events, marshalling and effectively allocating the capabilities of American society as a whole will be essential for national survival. Allocation of these capabilities will be especially challenging when, inevitably, requirements for assistance outstrip available resources. Moreover, the availability of these resources and capabilities will invariably be diminished by the effects of the Black Sky event. While supplementing the NRF will ensure that emergency managers become aware of prioritization criteria, broader outreach to the American public will also be helpful. Whole community engagement strategies and messaging should be modified accordingly to help strengthen citizen preparedness before Black Sky hazards strike, and support community-led response efforts when such events occur.
**Finding**

*Sustainment and restoration operations in a Black Sky event could potentially expose infrastructure owners and operators to lawsuits or penalties for regulatory violations.*

Government priorities will inform private sector sustainment and restoration efforts, but industry will be responsible for performing the operations. Harshly-prioritized sustainment and restoration measures by infrastructure owners and operators essential to saving lives may also carry liability risks.

**Recommendation:** *Government authorities should work closely with industry to pre-identify sustainment and restoration priorities, pre-script emergency orders, and provide legal and regulatory protection to infrastructure owners and operators as they execute those orders.*

The Fixing America’s Surface Transportation (FAST) Act,171 which amends the Federal Power Act, provides a valuable new vehicle for such collaborative efforts. The Federal Power Act grants the Secretary of Energy the authority to issue emergency orders to infrastructure owners and operators, and includes provisions for regulatory relief and cost recovery.172 The Department of Energy and its electric industry partners are currently examining how best to design these emergency orders and provide for associated regulatory and cost recovery mechanisms. As those efforts go forward, they should be tailored to account for EMP and other Black Sky hazards, each of which will require a different, threat-specific set of potential emergency orders.

---


172 Section 215A of the Federal Power Act grants the Secretary this authority. Prior to the FAST Act amendments, the Secretary had more limited emergency order authority under Section 202(c) of the FPA, which has been used in a number of instances (see: “DOE’s Use of Federal Power Act Emergency Authority,” Department of Energy, n.d.a., https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use). However, the FAST Act amends and expands Section 202(c) and creates Section 215A, providing the legislative basis for emergency actions in grid security emergencies.
2. State, Local, Tribal and Territorial Governments: Coordination with the Private Sector

In Building Operational Public Private Partnerships (July 2017), the National Emergency Management Association (NEMA) notes that state, local, tribal, and territorial (SLTT) leaders and emergency managers need the ability to coordinate with the private sector on infrastructure sustainment and restoration efforts. The report also emphasizes the need to prepare for coordinated cross-sector operations, with an emphasis on improving crisis information management capabilities.

However, NEMA also found that the U.S. lacks the unified guidance to build such coordination mechanisms. To address this gap, NEMA proposed the adoption of a repeatable process to tangibly and defensibly measure progress based on the DHS Incident Management Information Sharing (IMIS) Capability Maturity Model (CMM).

Business Emergency Operations Centers (BEOCs) can also provide a key organizational construct for public-private coordination. However, the report emphasizes that BEOCs and similar coordinating bodies “have languished largely because no guidance has been developed to facilitate development in at the least all 50 states, territories, and major metropolitan areas.”

The NEMA report provides a comprehensive set of recommendations on how to provide such guidance and enable cross-sector coordination with infrastructure owners and operators. To date, the existing Strategic Infrastructure Coordinating Council has focused primarily on building an integrated interface with the Federal government. In creating a Cross-Sector Coordinating Council for Black Sky preparedness, the Council should develop a mechanism to interface with SLTT governments. The NEMA recommendations provide a key starting point for doing so.

Industry leaders will need to significantly improve coordination with SLTT governments to facilitate successful cross-sector response operations in Black Sky events.

---

3. Organizing the Federal Government for Cross-Sector Infrastructure Operations

The same key documents that specify the goals and operational doctrine for response operations also lay out the organizational framework for Federal support in such efforts. As described by the NRF and its annexes, the Federal response system is carefully structured to facilitate coordination with infrastructure owners and operators. Indeed, in recent events such as Hurricanes Irma and Harvey, DOE noted that the level of coordination between power companies and government officials at the Federal (as well as local and state) levels was “remarkable.” Over 10,000 Federal staff representing 36 departments and agencies were on the ground for response and recovery efforts in Puerto Rico and the U.S. Virgin Islands.

However, as with response goals and doctrine, significant shortfalls exist in the ability of that Federal structure to support cross-sector infrastructure sustainment and restoration. Those gaps will be especially significant when Black Sky events put a premium on multi-agency support for cross-sector operations.

The analysis that follows examines a) the formal structure that the Federal government has established to incorporate industry leadership in response decision-making; b) how that system fared in Sandy, and subsequent efforts to improve government-industry collaboration; and c) additional opportunities for structural improvements by FEMA and its SSA partners.

a. The Current Federal Response System: Cross-Agency Coordination

The NRF notes that the President leads the Federal government’s emergency response efforts to ensure that the necessary resources are applied quickly and efficiently to catastrophic incidents. Given the scale of devastation that Black Sky events would create, and the importance of

---


infrastructure sustainment and restoration to saving and sustaining lives, those presidential leadership efforts could easily encompass outreach to the proposed CSCC.

Superstorm Sandy exemplified the benefits of presidential engagement with industry leaders. On October 30, 2012, President Obama participated in a call with electric utility executives to underscore the priority he attached to power restoration. He told the executives that he had ordered Federal agencies to eliminate any bureaucratic roadblocks that impeded utility restoration operations, and identified specific opportunities for Federal support.\(^\text{177}\) That presidential-level engagement continued and ultimately included a meeting with utility leaders to discuss how lessons learned from Sandy could be applied to future disasters.\(^\text{178}\)

However, in Black Sky events, Presidents will have multiple responsibilities competing for their attention. That will be especially true for EMP or cyber/kinetic attacks, where responding to the adversary and managing the escalatory process will be front and center among White House priorities. Top-level presidential engagement with the CSCC (supported by the National Security Council) could be very helpful in Black Sky events. However, to coordinate ongoing operations, the President will need to delegate down the authority to make decisions for Federal incident management.

*The Secretary of Homeland Security provides one option to exercise such delegated authority. HSPD-7’s grant of authority to the Secretary provides a strong rationale for selecting that option. The Directive states that:*

…the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts

---


\(^{178}\) Ibid.
among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.\textsuperscript{179}

The Secretary can also draw on an array of his or her Department’s organizations to help guide and coordinate infrastructure-related response operations. When disasters occur, DHS’s National Operations Center (NOC) serves as the principal operations center for the Department of Homeland Security and provides a common operating picture to support incident management, including data and assessments on disruptions to critical infrastructure.\textsuperscript{180} As will be discussed later in this section, organizations in DHS’ National Protection and Programs Directorate can also provide valuable analytic functions to support incident response.

Nevertheless, as with the President, the Secretary will still have many other responsibilities in a Black Sky event distinct from (and in potential competition with) overseeing and coordinating day-to-day response operations. The FEMA Administrator and other Agency officials are better suited to provide the sustained focus and emergency management expertise that Black Sky response efforts will require.

One key advantage of FEMA: the Stafford Act, the Post-Katrina Emergency Reform Act, and other laws provide the Agency with unique grants of authority to coordinate Federal support for industry sustainment and restoration efforts.\textsuperscript{181} For example, only the FEMA Administrator has the Stafford Act authority to “mission assign” the Department of Defense (DOD) and other agencies to provide support for infrastructure restoration.

---


FEMA is the Federal government’s focal point for accepting requests for disaster assistance from state governors, and for coordinating the Federal response to such requests. FEMA also has specialized Memoranda of Agreement and deep collaborative relationships with USACE, the Defense Logistics Agency, and other providers of critical Federal capabilities.

Especially important, FEMA leaders manage the National Response Coordination Center (NRCC), which coordinates overall Federal support for major disasters and catastrophic incidents. Most recently, FEMA stood up the NRCC for 10 days after Hurricane Maria hit Puerto Rico, with all ESFs activated, and daily teleconferences with leadership in various departments and agencies. The NRCC is designed to ensure that multiple Federal agencies can work in an integrated fashion, and can bring together all of the SSAs necessary for responding to Black Sky events. The NRCC can also include industry leaders in emergency management decision-making.

Taken together, these factors make the NRCC the best locus for Federal collaboration with the Cross-Sector Coordinating Council. However, lessons learned from extensive industry engagement in the NRCC during Superstorm Sandy provide cautionary lessons for making the NRCC the Federal partner for the CSCC.


b. Federal Coordination in Practice: Findings and Recommendations

As the severity of the power outage caused by Superstorm Sandy became evident, and emergency managers grappled with the impact of the outage on transportation systems, water utilities, and other infrastructure sectors, President Obama approved the first-ever deployment of an electric industry liaison to FEMA’s National Response Coordination Center.¹⁸⁴

David Owens, Executive Vice President of the Edison Electric Institute (EEI), served as the industry liaison for 10 days during the response to Sandy. EEI represents utilities that deliver 70% of the electricity in the United States, and played a key role in convening senior-level personnel from investor-owned utility members and other trade organizations. Owens served as the industry’s point-person to coordinate Federal support for utility restoration efforts on a nationwide scale (including military airlift of utility restoration assets from the West Coast to the affected region).¹⁸⁵

Moreover, at the President’s direction, FEMA stood up an Energy Restoration Task Force at the NRCC to provide for broader government-energy sector coordination. As fuel supplies and distribution became increasingly linked with access to power, the Task Force broadened its focus to address energy issues writ large.¹⁸⁶ Utility representatives also began embedding in regional and state Emergency Operations Centers (EOCs), creating a precedent in many such centers. In addition, electric utility CEOs participated in daily coordination conference calls with EEI representatives and DOE senior leadership to improve situational awareness and facilitate resource deployments.¹⁸⁷

¹⁸⁷ National Infrastructure Advisory Council (NIAC), Strengthening Regional Resilience through National, Regional, and Sector Partnerships, November 2013, p. 82.
Finding

NRCC response operations will need to formally include sustained, extensive industry participation far beyond that in any previous event.

The Energy Restoration Task Force achieved unprecedented success in prioritizing and delivering Federal support for utility-led restoration operations. However, because the NRCC had never before integrated such industry participation into response decision-making, officials from FEMA and other Agencies had to scramble to develop ad-hoc coordination mechanisms, communications links, and lines of authority. Their success in doing so reflected the extraordinary expertise and creativity of those who created the Task Force. But the disruptive effects of Black Sky events will make it implausible to create the necessary collaboration with industry “on the fly.” Moreover, because Black Sky events will inflict far greater damage on infrastructure than in Sandy or any other past event, the NRCC will need to engage industry leaders much more deeply in prioritized sustainment and response operations.

Recommendation: Infrastructure owners and operators and Federal officials should pre-arrange to include sustained industry representation in the NRCC.

When Black Sky events occur, organizational structures and coordinating mechanisms should already be in place to replicate the success of the Energy Restoration Task Force, yet also provide for much greater industry participation in real-time planning and execution of response operations. Exercises will also be essential to ensure that NRCC and industry personnel are prepared to effectively collaborate and have the pre-established personal relationships that are so valuable in emergency management.

188 Ibid., at pp. 82-84.
Finding

**Black Sky events will require the NRCC to coordinate with a far greater range of infrastructure sectors than in Superstorm Sandy.**

The Energy Restoration Task Force focused on restoration operations in the energy sector. Black Sky events will necessitate prioritized cross-sector sustainment and restoration operations and will therefore require Federal coordination with multiple sectors. The most obvious (and easiest to fix) implication of these requirements for expanded participation lies in NRCC office space. During Sandy, FEMA quickly found space adjacent to the NRCC for the Task Force staff. However, if a dozen or more critical infrastructure sectors need to be represented in the NRCC, such ad-hoc arrangements will be difficult to implement.

The lack of survivable communications systems will also present major challenges. During Sandy, Task Force members were able to communicate with their home companies and agencies unimpeded by the effects of the storm. In Black Sky events, extraordinary measures will be needed to provide for such communications. The BSX system will be able to provide for limited voice and data communications. Specialized FEMA communications systems may also be able to provide for at least some survivable communications between infrastructure owners, their representatives at the NRCC, and those conducting operations in the field. Nevertheless, the challenges of providing adequate industry-NRCC communications in Black Sky environments will be formidable and requires further analysis.

Hurricanes Harvey and Irma demonstrated the value of improved communications with industry in a relatively benign environment. DHS and FEMA led “cross-sector coordination calls,” in which the ESCC and representatives from other critical infrastructure sectors worked together to expedite restoration and address issues of interdependence – particularly between the electric and oil and natural gas subsectors. It is not clear, however, if this coordination occurred within the confines of the NRCC. Formalizing this structure and facilitating collaborative decision-making will be required to address the cross-sector challenges posed by Black Sky outages. So, too, will hardening communications systems so that they can withstand the catastrophic direct and cascading system failures that Black Sky hazards will create.
**Recommendation:** FEMA and the NRCC should pre-plan to provide work spaces for scores of infrastructure representatives and their Federal counterparts. They should also examine the extremely challenging communications requirements to support coordination from remote locations.

Depending on the day, over 20 personnel were at FEMA headquarters (where the NRCC is located) to staff and support the Energy Restoration Task Force. A significantly greater total number of industry personnel, spanning many critical infrastructure sectors, and their Federal partners will need work space to facilitate collaborative response operations in a Black Sky event. FEMA should arrange in advance to scale up its allocation of space for cross-sector coordination, and plan accordingly for the FEMA employees who will be displaced from their offices.

Given the scarcity of physical space, FEMA should also consider creating a collaborative virtual work space. The problem with doing so: Black Sky hazards will disrupt communications between industry representatives, their executive leadership, and operations personnel at remote locations (potentially over multiple FEMA regions). Sustaining data services will be a particularly difficult challenge. Further analysis is needed of the “bare minimum” voice and data functionality required to support industry contributions to NRCC decision-making and implementation, and how BSX and other survivable systems can help met those needs.

**Finding**

The division of responsibilities between the NRCC and SSAs presents a key design challenge for industry-Federal government coordination.

FEMA’s Hurricane Sandy After-Action Report (July 2013) noted that as power outages mounted, “FEMA senior leaders looked to ESF #12 (Energy)—coordinated by the U.S. Department of Energy (DOE)—to coordinate Federal efforts related to energy restoration.” However, “DOE struggled to meet this requirement and lacked the operational capability to fully engage supporting Federal departments and energy-sector partners in addressing energy-restoration challenges.” Those shortfalls prompted the establishment of the Energy Restoration Task Force at the NRCC.189

---

Since Superstorm Sandy, the Department of Energy has advanced an array of initiatives to strengthen its ability to execute its ESF-12 responsibilities. These efforts range from the creation of new systems to gather and share data for situational awareness (including EAGLE-I\textsuperscript{190}), to the development of a Comprehensive Emergency Management System to strengthen Department response and coordination capabilities.\textsuperscript{191} Senior White House officials also credited veteran emergency managers with experience from past disasters such as Katrina, Rita, and Sandy for an improved response in Irma and Harvey.\textsuperscript{192} However, persistent challenges with the response to Maria in Puerto Rico and the U.S. Virgin Islands highlighted opportunities for progress, especially in anticipation of multi-region Black Sky events.\textsuperscript{193}

Other Federal departments are also addressing their SSA responsibilities by strengthening their Emergency Operations Centers (EOCs) and capacity to coordinate with infrastructure owners and operators in severe events. The Department of Transportation, for example, now maintains a Crisis Management Center to constantly monitor the nation’s transportation systems and infrastructure, and to host the Transportation Secretary’s Emergency Response Team.\textsuperscript{194} Equivalent improvements in EOCs and other coordination mechanisms are going forward in agencies across the Federal government.

\textsuperscript{190} DOE's Environment for Analysis of Geo-Located Energy Information (EAGLE-I) system is a situational awareness tool which tracks and monitors outages and infrastructure assets by county, state and FEMA region. For more information, see: Liz Dalton, “DOE Announces Transition of EAGLE-I to Oak Ridge National Laboratory (ORNL), Taking Advantage of the Laboratory’s World-class Capabilities and Expertise,” Department of Energy, September 27, 2016, https://energy.gov/oe/articles/doe-announces-transition-eagle-i-oak-ridge-national-laboratory-ornl-taking-advantage.


These improvements are vital to helping departments meet their responsibilities as Sector Specific Agencies for infrastructure resilience. Ideally, in future events, it will never again be necessary to stand up the equivalent of the Energy Restoration Task force just because an SSA could not adequately respond to disruptions in their designated sectors.

However, SSAs are not nearly as well suited to coordinate cross-sector response operations with industry. While those agencies will undoubtedly be aware of the risks of cascading failures in Black Sky events, and mindful of the need for collaborative sustainment and restoration efforts with other sectors, they cannot mission assign other departments to contribute to such operations. Nor will they be receiving infrastructure-related requests for assistance from state governors under the NRF. Only FEMA and the NRCC are capable of meeting these requirements and integrating cross-sector industry input into broader emergency management decision-making.

**Recommendation:** Federal authorities should rationalize, standardize, and integrate the allocation of responsibilities and decision-making authorities among SSA EOCs and the NRCC.

Making department EOCs the focal point for coordinating emergency management operations with their respective sectors could, if carried too far, impede the NRCC’s ability to lead cross-sector operations. Yet, as SSAs, these departments also have strong industry ties and sector-specific expertise that FEMA and the NRCC will never be able to equal.

The best approach to Black Sky preparedness will be to leverage the comparative advantages of both the NRCC and SSAs. Federal departments should continue to strengthen their ability to provide situational awareness of disruptions to their sectors and be ready to analyze and present that data to the NRCC. The NRCC (including industry representatives from multiple sectors and departments) would then prioritize Federal support for industry-led sustainment and restoration operations. Federal and industry representatives at the NRCC would also make strategic-level decisions to integrate infrastructure operations with broader emergency management efforts, including mass care, when the scope of the incident affects multiple states and includes coordination with multiple governors. Departments and their infrastructure sector partners would then oversee the implementation of the NRCC’s decisions and report back on evolving and emerging requirements. The GINOM tool could be particularly useful for aggregating these requirements and supporting decision-making.
making to optimize response efforts. BSX could also be especially valuable to facilitate communication and situational awareness between the NRCC, SSAs, and relevant industry representatives given the extensive disruptions to traditional capabilities expected in Black Sky events.

**Finding**

*The National Infrastructure Coordinating Center can provide expanded support to the NRCC.*

In Black Sky events, government and industry leaders would benefit from advanced analytic and modeling support to assess infrastructure risks on an ongoing basis. As cascading failures evolve during such events, and unanticipated interdependencies emerge, emergency managers and industry leaders will need to continually reassess their response priorities. Data fusion and analysis, as well as a tool such as GINOM to support decision-making, will be vital to assist their efforts.

The National Infrastructure Coordinating Center (NICC) could help meet this need. Part of the National Operations Center at DHS Headquarters, the NICC receives situational, operational, and incident-related information regarding critical infrastructure from SSAs and other sources. A senior Federal official also noted that DHS is investing in a NICC readiness element that will enhance planning and exercise support at the national level, as well as relationships with SSAs and FEMA. The Office of Cyber and Infrastructure Analysis (OCIA) Integrated Analysis Cell (IAC), which is collocated with
the NICC, integrates and analyzes this data to support Federal incident management. The OCIA, along with the National Infrastructure Simulation and Analysis Center (NISAC) mentioned above, also lead DHS’ efforts to analyze cross-sector interdependencies and vulnerabilities. Going forward, there may be further opportunities to expand on NISAC’s contributions to pre- and post-event analysis in support of the NICC.

The NICC is supposed to collaborate closely with the NRCC. Recent disasters have provided opportunities for both organizations to make progress towards that goal. During Hurricane Matthew (2016), for example, the NICC provided regular updates on infrastructure at risk as the storm track evolved, and distributed this data to the NOC, sector-specific Information Sharing and Analysis Centers, and emergency managers. However, neither Matthew nor any other past event has required the NICC to provide the deep analytic support of cross-sector vulnerabilities and mitigation options that Black Sky events will necessitate.

**Recommendation:** DHS should make cross-sector analytic support of the NRCC a prime responsibility of the NICC, and resource the NICC accordingly.

The NRCC does not have adequate staff to provide predictive modeling of evolving interdependencies and risks of cascading, cross-sector failures. Rather than build such a staff, the NRCC should leverage the analytic expertise that already exists at the NICC, and exercise with the NICC (and with its industry partners) to ensure that infrastructure sustainment and restoration priorities can be continuously updated.

---

Finding

The role of FEMA’s National Business Emergency Operations Center (NBEOC) needs clarification.

FEMA established the NBEOC in 2012 to serve as a clearinghouse for two-way information sharing between public and private sector stakeholders in preparing for, responding to, and recovering from disasters. The NBEOC operates primarily on a virtual basis, using a range of web-based platforms and dashboards to coordinate with members.196 FEMA activated the NBEOC for nearly three weeks as part of the NRCC in Superstorm Sandy, coordinating with a membership group that nearly doubled in anticipation of the storm.197 FEMA’s Sandy AAR found that the NBEOC provided situational awareness to the private sector, responded to private sector inquiries, and identified and resolved critical private sector needs and issues.

However, the Sandy Report also found that some government and private sector partners were unclear about the distinction between NBEOC functions and the responsibilities of the NICC.198 The NICC is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of U.S. critical infrastructure for the Federal government.199 Cascadia Rising (2016) and other recent exercises indicate that the respective roles of these two organizations remains unclear, creating confusion in the private sector as to which one is the appropriate focal point for information sharing.

---

Recommendation: Rather than replicate the functions of the NICC, FEMA and its partners should consider how the NBEOC could perform other, high-priority missions.

One option would be to help solicit and coordinate private sector support to meet survivor and emergency response personnel needs for food, housing, and other assistance. The NBEOC displayed progress in this regard in the response to the 2017 hurricanes, successfully working to coordinate private sector shipments of food and basic resources in Irma and Harvey,200 and later Maria.201 In contrast, as proposed above, the NICC should play a crucial role in supporting the NRCC by analyzing cross-sector risks and mitigation priorities in Black Sky events.

FEMA and its partners should consider other options to help define the NBEOC’s role as well. In particular, FEMA should take the NBEOC and associated private sector activities out of the Agency’s External Affairs directorate and integrate it with FEMA planning and operational functions to reflect the Center’s operational role in catastrophic events.202

---


202 National Emergency Managers Association (NEMA) and the International Association of Emergency Managers (IAEM), Harvey Response Private Sector Integration: Lessons for Irma and Beyond, n.d.a., p. 6.
B. State Leadership for Cross-Sector Infrastructure Operations

State governors will be crucial to emergency response in Black Sky outages. Indeed, the National Response Framework notes that “states are sovereign entities, and the governor has responsibility for public safety and welfare.”\textsuperscript{203} To strengthen coordination between government and industry for cross-sector operations, enabling the NRCC to serve as the partner for the proposed Cross-Sector Coordinating Council (CSCC) will constitute only one line of effort. A second set of initiatives will be required to provide for state leadership in this system and to manage competing state priorities for infrastructure sustainment and restoration operations in Black Sky events.

1. Unified Coordination: State EOCs, Joint Field Offices, and Supporting Organizations

Every state maintains an EOC to help manage incidents and coordinate local and state agency operations. Recognizing the critical role of infrastructure restoration in incident management, a growing number of states reserve seats in their EOCs for energy sector representatives to participate in emergency decision-making. Black Sky operations will require representation from many more sectors. However, many state EOCs are small and lack the capacity to add such industry personnel. In the State of Washington, for example, the state EOC policy room (where many key resource allocation decisions will be made) has a total of only 19 seats.\textsuperscript{204} Providing for secure communications between EOCs and infrastructure owners and operators will be essential to facilitate coordination despite these space constraints.

Black Sky events, of course, will overwhelm the response capabilities of individual states and their infrastructure restoration assets. In the electric subsector, the water sector, natural gas subsector, and other sectors, robust systems of mutual assistance enable utilities in neighboring states to assist the

stricken region. The Emergency Management Assistance Compact (EMAC) system enables governors to share National Guard resources across state lines to support infrastructure restoration.\textsuperscript{205} EMAC also helps states share public sector resources under the authority (and liability) of the issuing governor. Nearly 40 states jointly deployed over 12,500 personnel through the EMAC in response to Hurricanes Harvey, Irma, and Maria, supporting incident management, temporary sheltering, law enforcement, public health, emergency operations centers, debris removal, water purification, and more.\textsuperscript{206} States also provided EMAC liaisons to work with FEMA in Regional Offices, and coordinate assistance efforts in the NRCC. Coordinating these multiple state and industry response operations and integrating them with Federal assistance will present a monumental challenge in Black Sky events.

“Unified Coordination” will be essential to meet this challenge. Under the NRF, Unified Coordination is typically directed from a Joint Field Office (JFO), a temporary Federal facility that provides a central location for coordination of response efforts by the private sector, NGOs, and all levels of government. The JFO is the field-level focal point for Federal officials to consider, adjudicate, and act upon requests for Federal assistance. Within the JFO, a Unified Coordination Group (UCG) is composed of senior leaders representing state, tribal, and


\textsuperscript{206} “EMAC FLEXES TO RESPOND TO HISTORIC HURRICANES,” National Emergency Management Association, October 6, 2017, E-mail Press Release.
Federal interests and, “in certain circumstances,” the private sector – all of whom must have the jurisdictional responsibility and authorities needed to help guide response decision-making.²⁰⁷

**Finding**

*Governors will continue to be vital in leading response efforts for the citizens of their states.*

Under emergency response doctrine and, more importantly, the U.S. constitution, governors are responsible for the health and safety of their constituents. Black Sky events will put a premium on governors’ ability to lead the overall state response to catastrophes, coordinate with the Federal government and private sector, and prioritize requests for assistance within their state.

**Recommendation:** *Governors, their staffs, and state emergency managers should collaborate closely with industry on pre-planning efforts to help meet state infrastructure sustainment and restoration priorities.*

As with Federal leadership, extensive pre-event coordination with infrastructure owners and operators will help governors conduct oversight of industry-led emergency response operations in their state.

State, local, tribal, and territorial (SLTT) emergency management officials should also observe and potentially provide input on the creation of the Black Sky Prioritization List in order to ensure that they maintain accurate assessments of critical facilities and functions in their respective states and regions. As observed below, this may contribute to consensus-building on interstate prioritization and competition for resources. SLTT officials should also participate in Black Sky Playbook development initiatives where applicable.

Finding

The inclusion of industry representatives in the Unified Coordination Group will be imperative for Black Sky events.

The NRF notes that UCG composition will vary from incident to incident depending on the scope and nature of the disaster. Given the importance of prioritized infrastructure sustainment and restoration in Black Sky events, UCGs will be unable to provide for effective event coordination unless they include representatives of infrastructure owners and operators. However, in past disasters, no UCG has provided for such large-scale industry participation.

Recommendation (a): Pre-plan for industry representation in UCGs and exercise government-industry coordination.

Given the lack of experience in including infrastructure representatives in UCGs, state and Federal emergency managers should collaborate with the proposed CSCC to determine in advance how that representation should be structured. Ideally, consistent with current UCG guidelines for participation, infrastructure representatives should have the authority to make or convey resource allocation decisions on behalf of their respective sectors. Use of this new UCG construct in National Level Exercises (NLEs) and regional equivalents will be essential to identify opportunities for improvement and build collaborative experience.

Recommendation (b): Clarify support roles for DHS infrastructure experts assigned to field organizations.

Under the Federal Incident Response Plan, DHS Infrastructure Liaisons are supposed to serve as the principal advisor to the UCG regarding all national, regional, and cross-sector critical infrastructure-related issues, including recommendations on the prioritization of critical infrastructure within the affected area. A senior Federal official noted that DHS is investing more in planning, exercise, and analytic efforts to better support the Infrastructure Liaison role. DHS Protective Security Advisors (PSAs) are also supposed to serve as incident management personnel and liaisons in state and local EOCs.208

However, as with the NICC, exercises will be essential to ensure that these field personnel can meet the unprecedented cross-sector challenges that multi-region Black Sky events will create. Federal and industry leaders will also need to ensure that the NRCC remains the locus of strategic-level, multi-region decision-making, and avoid the risk that field personnel will offer conflicting guidance on sustainment and restoration priorities.

2. Managing Potential Conflicts between State Priorities

When New York State and New York City gave emergency managers competing guidance on water pumping priorities for tunnels in Superstorm Sandy, those disagreements only hinted at the challenges to come in Black Sky events. Such events will inflict catastrophic damage to infrastructure across multiple states. In deciding which sustainment and restoration operations will go forward first, emergency managers and their industry partners will be at risk of inviting harsh criticism from governors, each of whom can be counted on to put the needs of their own states above others. This interstate competition has been an issue in less catastrophic events. For example, in the 2010 Deepwater Horizon oil spill response, the National Incident Commander of the Unified Command Admiral Thad Allen noted that competition for containment boom was “almost a political litmus test on federal support,” and this phenomenon became known as the ‘Boom Wars’ within the Unified Command. Interstate and intrastate competition will be particularly intense in Black Sky events, where severe outages will impact an unprecedented number of states.

Building consensus support for the Black Sky Prioritization List among state leaders will help manage such challenges. If governors and their senior advisors have the opportunity to review that list, receive briefings on the analysis that supported its development, and nominate additional state-level assets for

---

inclusion, they may be more likely to support the use of the BPSL to prioritize infrastructure operations in multi-state events. Ultimately, it will be critical to pre-identify and embed SLTT priorities into sustainment and restoration plans before Black Sky events occur. Doing so once they are underway will be vastly more difficult, if not impossible.

However, especially for states with few assets on the List, governors concerned for the safety of their citizens and the survival of their economies will be calling the White House and the FEMA Administrator to advocate on behalf of their own infrastructure priorities. Governors may also pressure infrastructure owners and operators in their states to ensure that in-state restoration operations go forward, even if higher national-level priorities exist elsewhere. In Sandy, problems emerged in winning governor approval to have utility crews flown out of state to support mutual assistance agreement operations. Black Sky events – especially those in which re-attacks with cyber weapons are possible – will create still greater strains on the willingness of governors to support sending industry resources to other states. While natural disasters such as Superstorm Sandy and the 2017 hurricanes allow large numbers of utility workers from non-affected areas to help restore power, a cyber event will necessitate drawing on a much smaller pool of subject matter experts with the required individual system expertise and trust of affected utilities. Given the potential for re-attack across a geographically dispersed area, utilities may also be more reluctant to loan their services.

Finding

_The FEMA Administrator is best positioned to resolve conflicting state priorities._

While the President will ultimately bear responsibility for the Federal government’s resource allocation decisions, Black Sky events (especially those resulting from catastrophic attacks) will require the President to lead decision-making on multiple issues. The responsibility for fielding calls from multiple U.S. governors should be delegated down to the FEMA Administrator. Under

the NRF, the Administrator is responsible for receiving and coordinating the Federal response to state-level requests for assistance. Making the Administrator responsible for deciding between competing requests (and, inevitably, denying some of them) could also help insulate the President from political pressure and enmity. For both reasons, the FEMA Administrator is best positioned to manage conflicting state priorities.

**Recommendation:** *FEMA should staff up to support sustained engagement with multiple governors.*

In Sandy, former FEMA Administrator Craig Fugate did a masterful job of managing requests for assistance from a handful of governors, from both political parties and just prior to a presidential election. However, Black Sky events will likely inflict catastrophic damage on dozens of states simultaneously. Moreover, in Sandy, FEMA and its partners resolved most assistance resource allocation decisions within two weeks. Black Sky events will demand much longer-term engagement with state leaders. As FEMA is currently staffed and structured, those engagement needs would prove overwhelming. The Agency should build plans and capabilities to prepare for the “worst case” requirement to conduct resource allocation discussions with all 55 governors of U.S. states and territories.

---

**Finding**

*There will be immense “political heat” for prioritized industry sustainment and restoration operations.*

Public messaging by elected officials will be essential to support prioritized sustainment and restoration operations. When infrastructure owners and operators protect national security by focusing on support for military bases and other security assets, they should not bear the burden of explaining that focus to angry customers, much less to mayors and governors clamoring for support for their citizens. Instead, elected officials should be prepared to “take the heat” on behalf of infrastructure leaders. Moreover, well before Black Sky events occur, these leaders should explain to their constituents why some areas will be sustained and more rapidly restored than others.

**Recommendation:** *Federal, state, and local leaders should develop messaging plans and capabilities to account for delayed service restoration.*
This chapter has already identified the need for public messaging to explain why and how infrastructure operations are being prioritized, especially for citizens facing extended service disruptions as a result. As part of that effort, ensuring unity of messaging between industry and elected officials at all levels of government will help support Black Sky operations. Doing so will not be easy: competing sustainment and restoration priorities are bound to emerge. Pre-event exercises and planning will be essential to help manage these disagreements in the face of intense political pressure and citizen concerns. Developing “unity of messaging” coordination mechanisms between industry and government will also be essential.

C. Revamping the Emergency Support Function System for Cross-Sector Infrastructure Operations

Under the NRF, the Emergency Support Function (ESF) system is a coordination structure used by the Federal government for building, maintaining, and delivering response capabilities, including those necessary for sustaining and restoring critical infrastructure. The NRF notes that these ESFs “have proven to be an effective way to bundle and manage resources to deliver” such capabilities.\textsuperscript{211} ESFs have long been incorporated into NRCC and JFO operations. Moreover, many local, state, and tribal jurisdictions have adopted and tailored the ESF system to help coordinate their own response efforts. That nationwide adoption has also helped make the ESF system the basic framework for sharing state capabilities in Emergency Management Assistance Compact operations.

Appendix A lists the Federal ESFs that support response efforts, the Federal departments and agencies responsible for coordinating them, and the core response capabilities they entail. Federal agencies that serve as ESF

coordinators do more than help manage the delivery of Federal resources in response operations. The coordinators and their partners also conduct training and exercises to strengthen their core operational capabilities. They monitor stakeholders’ progress in building capacity and help lead planning and preparedness activities focused on their specific emergency functions.

The nationwide use of the ESF system and the range of preparedness initiatives it encompasses could make the system uniquely valuable as a basis for coordinating the delivery of resources and capabilities to support industry-led infrastructure operations.

Capitalizing on that opportunity in Black Sky events will require the ESF system to address three of its critical shortfalls by:

1. Integrating the private sector in ESF activities;
2. Building preparedness for wide-area, catastrophic damage and disruption of critical infrastructure; and
3. Transcending the sector-specific construct of the ESF system to facilitate cross-sector sustainment and restoration operations.

**Finding**

*ESFs are focused primarily on the delivery of government response capabilities and are poorly structured to help coordinate industry-government collaboration.*

Since its inception, the primary focus of the Federal ESF system has been to coordinate interagency support for Federal responses to an incident.\textsuperscript{212} The NRF notes that the Federal agency coordinators for each ESF are responsible for coordinating with their corresponding private sector.\textsuperscript{213} However, the Framework provides no additional detail on what such coordination should encompass or how it should be achieved. Far too many ESFs remain government-focused; with the exception of ESF-12 (Energy) and a handful of other functions, they do not entail sustained engagement with leading


companies in their respective sectors. Moreover, a former state Director of Homeland Security & Emergency Management noted that the ESFs are not sufficiently organized, trained, or prepared for collaborative problem-solving and decision-making, often focusing solely on carrying out narrowly-defined mission assignments.

**Recommendation:** Federal ESF coordinators should update their respective ESF Annexes to include specific goals and coordination mechanisms for integrating industry into ESF activities.

The Emergency Support Function Leaders Group (ESFLG) is ideally suited to strengthen industry participation in the ESF system. The ESFLG comprises the Federal departments and agencies that are designated as ESF coordinators or coordinating agencies for other NRF annexes. FEMA leads the ESFLG and is responsible for calling meetings and other administrative functions. The ESFLG provides a forum for departments and agencies with roles in Federal incident response to jointly address topics such as policies, preparedness, and training.214

The ESFLG should assess the degree to which industry representatives and key companies are included in planning, exercising, and response coordination mechanisms under each ESF. Industry leaders should self-organize to determine how they will be represented within their respective ESFs. The Administrator should also collaborate with SSAs to capture emerging best practices from ESF-12 and other functions that already have strong private sector collaboration, so that other SSAs can modify and apply those practices to meet their own ESF-specific needs. Similar collaborative efforts should go forward at the state level with infrastructure owners and operators in those states.

**Finding**

*ESFs should emphasize preparedness against catastrophic events.*

The January 2008 Introduction to Emergency Support Function Annexes emphasizes the need for ESF coordinators to focus on “activities relating to catastrophic incident planning and critical infrastructure preparedness, as

---

214 Ibid., at p. 39.
appropriate.” However, the NRF no longer includes that mission in the Framework’s description of ESF functions.

A regional study ahead of the 2011 National Level Exercise found that Federal ESFs had given no consideration to the sizeable gaps between the resources and capabilities available at the state level and what would be required in response to a catastrophic event. Moreover, many ESFs define their primary functions in ways that do not adequately specify their responsibilities for missions that will be crucial for responding to Black Sky events.

Emergency Support Function 11, Agriculture and Natural Resources, provides a case in point. The January 2008 version of that ESF Annex noted the U.S. Department of Agriculture (USDA) is responsible for ensuring “the safety and security of the commercial food supply,” and “the availability and delivery of food products” to support incident management. In particular, USDA “identifies, secures and arranges for the transportation of food to affected areas, and supports mass care by providing food for shelters and other mass feeding sites.” But nothing in the ESF Annex summarizes what these tasks will entail in catastrophic events, when the handful of food distribution centers that serve “big box” and supermarket chains in major cities will experience severe disruption to their refrigeration, transportation, and delivery operations.

The update of ESF-11 in June 2016 provided an opportunity to include additional details on incident response. Instead, the 2016 version takes a step backwards. The updated ESF Annex calls for USDA to coordinate with other responders to determine the nutritional needs of the affected area and develop plans to ensure food distribution. But the 2016 version eliminates all reference to commercial food supply issues in disasters, and (apart from ensuring “the safety and defense of the nation’s supply of meat, poultry and processed egg products”) fails to address the food distribution and security missions that will vital in Black Sky events.

216 Central United States Earthquake Consortium, CUSEC After-Action Report (AAR), December 2011, p. 34.
**Recommendation:** As Federal ESF coordinators execute their responsibilities for planning and exercising, they should focus on catastrophic response requirements.

The Power Outage Incident Annex, which will support the development of regional planning under ESF-12, exemplifies the opportunity for ESF coordinators and their partners to focus on the mission requirements of extreme events. The ESFLG should encourage and facilitate such planning efforts across all ESFs. Industry leaders should also consider sharing their Black Sky Playbooks with the ESF Agency coordinators in their sectors.

---

**Finding**

The ESF system is too “stovepiped” to facilitate cross-sector sustainment and restoration operations.

By design, Emergency Support Functions focus on specific response tasks and (in many cases) particular infrastructure sectors. That focus has been enormously helpful for building sector-specific plans and capabilities for responding to events and coordinating the delivery of government capabilities to execute ESF missions. However, the ESF system is poorly structured to facilitate the cross-sector industry infrastructure operations that will be essential in Black Sky events.

In FEMA’s After-Action Report (AAR) for Superstorm Sandy, the Agency found that while ESFs are supposed to draw upon the response assets of multiple Federal departments, the Sandy response “revealed that several ESF coordinating agencies have adopted a more department-centric approach to response operations, rather than the integrated functional approach prescribed by the NRF. In these instances, ESF coordinating agencies did not fully draw upon the capabilities of supporting departments and agencies.”219 Enabling ESF coordinators to collaborate with infrastructure owners and operators beyond their own sectors will be still more challenging – and absolutely vital against Black Sky hazards.

---

Recommendation: The ESFLG should establish a new ESF, Emergency Support Function 14 (Cross-Sector Infrastructure Coordination), to meet the challenges created by infrastructure interdependence and cascading failures.

One way to strengthen Black Sky preparedness would be to require each ESF to identify and account for cross-sector vulnerabilities. Such efforts have already begun in some ESFs and should be advanced system-wide.

Such cross-ESF operations would benefit from specialized, sustained efforts to meet the challenges they pose. One of the reasons that the ESF system has been so successful is that each ESF coordinator has been able to help focus training, exercising, and planning on their respective functions and infrastructure sectors. A similar, dedicated effort by each ESF to prepare for and enable cross-sector operations could contribute to Black Sky resilience.

However, to truly embed cross-sector response operations in the ESF system, industry and government leaders should consider establishing an Emergency Support Function dedicated to cross-sector coordination.

ESF-14 is “vacant;” it was once allocated to incident recovery, but recovery functions have since moved to a separate National Disaster Recovery Framework and planning system. Dedicating ESF-14 to cross-sector coordination would provide the best possible use of that function to strengthen Black Sky preparedness.

The eventual coordinator for ESF-14 should consider using EIS Council’s Systems Engineering methodology as a means to improve cross-sector coordination. This approach tasks each sector with setting response goals, establishing Black Sky service levels, identifying internal requirements, and explicitly specifying external (cross-sector) requirements. These individual sector Black Sky Playbooks provide an excellent foundation for cross-sector exercises such as EARTH EX, and constitute a matrix for evolving to an end-to-end, top-to-bottom, holistically-integrated response management decision support capability such as GINOM. This evolution can spur progress in catastrophic incident resilience.

CHAPTER TWO

THE BLACK SKY EMERGENCY COMMUNICATION AND COORDINATION SYSTEM (BSX™)

Assessing Communication and Coordination Requirements for Complex Catastrophes
I | INTRODUCTION

Building the collective capacity to effectively handle large-scale power outages and other complex catastrophes requires many simultaneous lines of effort from public and private sector stakeholders. As indicated in Chapter I, carefully integrated planning across the many interdependent critical infrastructure sectors and their partners at all levels of government will be critical.

Building coordinated, prioritized multi-sector strategies for critical resilience investments will be an important part of this planning, and must be implemented well before a Black Sky event. Similar coordination will also be required to guide infrastructure restoration and population sustainment after catastrophe strikes. However, in disasters on this scale, all normal telecommunications, internet, and related services will fail. As a result, infrastructure sustainment and restoration operations will not be possible. This represents one of the most fundamental challenges faced by modern nations. If not addressed aggressively, the U.S. risks unprecedented infrastructure failures and the breakdown of societal continuity.
The classic scenario faced by planners addressing extreme events is a subcontinent-scale power outage. Such blackouts, especially when caused by malicious threats like cyber or EMP attacks, could be associated with extensive and widely-distributed damage to power grid facilities. Given the scale of such outages, this damage will take significant time to assess and repair. Power restoration after such an outage will require “black start,” a largely manual process which, given the inevitable disruption and likely damage in such a large-scale outage, will take time.

In a Black Sky event, black start power restoration will take – at best – weeks, or longer, to implement, and will only be possible if adequate, broadly-distributed and interconnected emergency telecommunications are available to host that process. Without such communications capabilities, the process could take months or years. Meanwhile, other multi-sector efforts essential to sustain the minimal resources and services needed for population sustainment will rely on precisely the same capabilities.

If modern nations wish to be capable of surviving large-scale complex catastrophes, implementing a widely-distributed, Black Sky-compatible emergency communication and coordination system is the first, most fundamental requirement they must address.

A Black Sky-compatible emergency communications system represents a fundamental, enabling capability or toolset, without which all other planning for severe, large-scale emergency scenarios will not be implementable.

1. Communication

As reviewed in Chapter I, large-scale, long-duration power outages can only be surmounted by new approaches to prioritized resilience investments, and by adapting existing coordination structures to span the unprecedented needs such events will have for cross-sector planning and operational coordination. Yet, as described below, power outages of this scale will also result in the failure
of most or all normal telecommunications systems throughout the affected area. Such new multi-sector coordination approaches will not be viable without communications systems that can survive a Black Sky event, and even under such circumstances, interconnect nearly all sectors, including key segments of their supply chains.

Developing, implementing, and deploying such a system – designed to survive a long-duration outage and continue to operate without depending on a functional power grid or normal, national telecommunications assets – is a fundamental test of the credibility of a nation’s national continuity planning and national security, as broadly defined in the 2017 U.S. *National Security Strategy*.1

2. Coordination: Situational Awareness and Multi-Sector Modeling and Simulation

Without grid power and communications, our infrastructure and resource networks – the interdependent, tightly-linked systems that generate and distribute the resources needed to support power restoration and sustain populations – will fail, precisely when they are needed most.

A widely-distributed, self-powered emergency communications network will therefore be essential in Black Sky outages. However, the multi-sector coordination authorities to whom this capability will be particularly critical will need help to enable “manual” sustainment and restoration operations for a critical subset of those infrastructure and resource networks.

Given the scale of effort required to support multi-sector infrastructure restoration and sustain modern megacities, this help – which may also be

1 The National Security Strategy of the United States of America (December 2017) employs an all-encompassing definition of national security that goes beyond the nation’s fundamental military challenges. In contrast to national defense, this definition includes threats to critical infrastructure and critical supply chains, the economy, intellectual property, etc. See: President Donald Trump, *National Security Strategy of the United States of America*, December 2017, p. 1.
characterized as “machine assistance” – will need to include approaches to provide several additional tools and capabilities, including:

- Adequate situational awareness
- Multi-sector modeling and “mapping” of cross-sector interdependencies
- The multi-sector simulation and forecasting that will be essential to provide decision support capabilities

And since each of these tools will themselves require widely-distributed, real-time communications connectivity, they will need the same type of Black Sky-compatible emergency communications system to host their operation and provide a seamless user interface for users and decision makers. This chapter reviews examples of tools that provide these capabilities, the Situational Awareness Network Diagnostic (SAND™) System and the Global Infrastructure Network Optimization Model (GINOM™)², in the context of the Black Sky Emergency Communication and Coordination System (BSX™) designed to host their operation.

---

² For more information on the SAND™ and GINOM™ initiatives, please write to info@eiscouncil.org.
3. Developing an Emergency Communications Tactical Network:
   Working Toward a National-Scale All-Hazard Emergency Communications System and Tactical Network, Interoperable with Existing Emergency Communications Systems

The viability of the new initiatives and organizational realignments proposed in the previous chapter will depend on a widely-distributed and interlinked communication and coordination system that can survive a Black Sky event. This system must be able to operate for weeks or months in the absence of grid power. It will also need to operate without depending on the national telecommunications backbone, which will fail in a long duration grid outage.

Of course, multiple public and private sector emergency communications systems already exist to support disaster operations. In many sectors, infrastructure owners and operators are improving the diversity and survivability of these systems. Government emergency communications systems for disaster response (especially those managed by FEMA and the National Guard) are also becoming more resilient. Typically, however, private sector systems are structured to sustain connectivity with an organization’s own facilities, critical assets, and subsector partners. In Black Sky events, nearly all organizations will need support from many interdependent sectors to sustain even minimal service, support infrastructure restoration, and contribute meaningfully to population sustainment operations. At present, where independent emergency communications systems are available, they have little capability for interoperability.

Emergency communications systems maintained by the National Guard and other governmental organizations suffer from an equivalent shortfall. These systems are focused on serving government users. They rarely provide direct links to infrastructure owners and operators and essential resource and service providers, even though infrastructure sustainment and restoration will be the most important factor for saving and sustaining lives in Black Sky events.
Nor are most existing communications systems – whether the regular societal systems, or the localized emergency systems described above – equipped to operate for a month or more in the absence of power from the electric grid. And after some period of time – certainly less than 72 hours – the back-up power systems for the “normal” national telecommunications backbone (e.g., the internet, landline and cellphone systems, and the ground segments of satellite communications systems) will run out of power and shut down. Even satellite phones will not operate indefinitely in the absence of power at the satellite control stations.

4. Looking Ahead

Given the increasing interdependence of infrastructure sectors, and the broad array of public and private sector partners essential to help sustain and restore essential services, deploying a Black Sky-compatible communication and coordination system to all critical sectors, key partners, and relevant supply chains will be vital to prepare for extreme events. To be effective, such a system must be interoperable with any available emergency communications systems, including those of the military, police, first responders, and security personnel.

Our analysis has indicated that a fully-deployed Black Sky emergency communications system would need to include approximately 200,000 nodes across the United States. The system could therefore also be used as a limited, emergency-oriented data network (at much lower bandwidth than conventional societal systems), sufficient for the early stages of sustaintment and restoration operations following a Black Sky event. As deployment increases and node-to-node ranges decrease across the mesh network anticipated for such a system, the system could incorporate shorter-range, higher-bandwidth components to provide capabilities comparable to a limited “emergency internet.”
5. Hosting an Emergency Financial Accounting System

One of the most fundamental needs for a Black Sky-compatible emergency communication and coordination system in a complex catastrophe scenario would be to support an emergency financial accounting system. Given the inevitable, severe disruption of normal monetary institutions and networks, a backup financial strategy will be essential to allow for continuity of the critical backbone of commerce needed to support utility restoration, and to save and sustain lives. As corporations, banking institutions, and government stakeholders consider emergency credit liquidity concepts and other approaches to develop an emergency monetary system, very broad multi-sector communications connectivity and coordination support will be essential. The BSX™ system, described in detail in this chapter, can provide such connectivity and coordination.

6. The Black Sky Emergency Communication and Coordination System (BSX™): An example of a Black Sky-compatible system architecture

This chapter provides an analysis of the BSX system, whose design is currently being developed by the Electric Infrastructure Security Council. Making use of technologies originally invented for the U.S. Army’s highly-successful Blue-Force Tracker Command, Control, and Communication System, BSX nodes will be configured to operate with or without externally supplied power,³ and without external communications or other infrastructures, supporting national-scale interconnection of approximately 200,000 nodes.

³ Power supplies for BSX nodes will vary depending on the site at which it is situated. Many critical facilities will be developing plans and capabilities to sustain the supply of emergency power (and thereby facilitate continued operation) in extended outages. This can be accounted for in the deployed BSX configuration for such installations, as BSX nodes will rely on these capabilities where possible. BSX sites without adequate emergency power supplies can choose from a range of potential power module configurations. This issue is examined in detail in Section IV (D).
Fundamentally, BSX is a scalable system architecture, utilizing an intelligent director-enabled mesh network configuration to support the unique capabilities needed for Black Sky communication and coordination. This gives the system a robust capability to incorporate a wide range of communication components, and to evolve to stay current with the best available technologies.

It is designed to operate as a standalone emergency communications system, and to provide connectivity with any existing emergency communications systems that survive a Black Sky event. This allows BSX to act as a “bridge,” providing for inter-communication between these previously incompatible emergency communications systems.

Now in the early stages of prototype development, BSX will perform three critical functions following Black Sky events.

a. **Essential BSX System Functions**

- **Nationally Deployed, All-Sector Emergency Communication:**
  Provide voice and data communications to enable infrastructure support, population sustainment, and response operations, as well as other Black Sky activities.

- **Hosting a Situational Awareness Hub**
  BSX will be able to host operation of the Situational Awareness Network Diagnostic (SAND™) System, now in initial development. SAND is designed to remotely acquire diagnostic data from both current and newly deployed sensors embedded in critical infrastructure, resource, and service sectors and their supply chains. This critical capability
provides a unique multi-sector, real-time view that will be essential for decision makers in Black Sky events.

- **Hosting a Multi-Sector Model and Simulation**
  BSX is also designed to host operation of the Global Infrastructure Network Optimization Model (GINOM™). GINOM is a software-driven, multi-infrastructure modeling and simulation framework. Such a system will be essential to assist decision makers in all sectors, as they work to “manually” support the wide array of (normally self-sustaining) resource flows needed to enable infrastructure restoration and sustain the affected population. Given the complexity of this task, interdependency mapping and artificial intelligence (AI) support from GINOM will be essential to help guide these managers to optimize prioritized, time sensitive decisions in responding to the vast array of unpredictable events and the many dimensions of intricate challenges that will emerge in complex catastrophes of this magnitude.  

b. **BSX System Design Summary**
  BSX is an interoperable, Black Sky hazard-protected emergency communication and coordination system designed to operate without requiring connectivity to the nation’s telecommunications networks. Designed with an array of options to ensure adequate off-grid power at all nodes for 30-60 days of operation, BSX is designed to easily interconnect with and supplement available organization-specific emergency communications systems, supporting ubiquitous, multi-sector deployment of 200,000+ nodes across the United States, and, over time, similar deployments internationally.

---

4 The “BSX resource family” includes both the BSX™ system itself and the Global Infrastructure Network Optimization Model (GINOM™) initiative, a multi-sector model providing both interdependency mapping and AI-enabled simulation and forecasting capabilities. GINOM also includes: 1) the Situational Awareness and Network Diagnostic (SAND™) system providing multi-sector, real-time status information; and 2) the Complex Adaptive Network Optimization Engine (CANOE™), providing iteratively reoptimized recommendations to decision makers, based on an AI-enabled layer of the GINOM system. These initiatives will be described in greater detail in subsequent EIS Council publications.
The BSX system, communications protocols, and network management software will be designed and maintained to support evolving requirements for interconnected, Black Sky operations spanning all infrastructure, critical resource supplier, and mass-care NGO sectors, as well as state and Federal emergency management agencies and a range of other government organizations. The deployed BSX network and its subnets will provide ubiquitous, all-sector voice and limited data rate connectivity to support the critical, initial stages of emergency response, infrastructure restoration, and population and environment sustainment following wide-area regional blackouts (when most or all other national communications systems will typically be unavailable).

BSX development is planned to occur in stages, beginning with initial, Block I Limited Operational Capability (LOC) deployment for selected corporate and government customers. Designed to support initial voice operations and limited data transmission, Block I is being rolled out to a limited number of early adopters. Knowledge gained from Block I LOC will be leveraged to improve the BSX network, with future stages supporting advanced situational awareness and decision support capabilities. To this end, future deployments will host the SAND™ all-sector Black Sky situational awareness framework, with a network configuration designed to support and enable the evolving GINOM™ all-sector simulation model that will provide both multi-sector interdependency mapping and an AI-driven, real-time decision support engine for use in complex catastrophe scenarios.

The system uses a mesh, internet-like network configuration adapted for the special conditions of long-distance radio, providing communication path flexibility and high reliability voice and data communication.

As the BSX system’s deployment expands, or if deployed node density is increased in selected, key areas, data rates will also expand, enabling
the system to offer added capability. Ultimately, especially in urban areas with high node densities, higher data rates will enable operators to use the evolved BSX network as a Black Sky Emergency Internet, giving users access to a searchable emergency network, including specially-designed emergency network websites which can operate under all-hazard conditions.

![A preliminary version of a BSX controller interface, displayed in EPRO SECTOR Winter, 2017 at PJM Headquarters, Audubon PA.](image)

c. **Current Status of the BSX System**

In 2017, EIS Council and its partners, Neil Siegel, LLC, and Applied Minds, LLC, completed architecture development and conceptual design of the BSX System. Key elements of a system prototype were developed in support of the Electric Power Research Institute's Emergency Communication Research Project. These key elements and their capabilities were successfully demonstrated at the EPRO SECTOR Executive Committee Winter 2017 meeting at PJM Interconnection Headquarters in December 2017.

The next step in the development of this multi-sector system will be BSX Block I Limited Operational Capability (LOC) Build deployment. This entails building interconnectable, near full-scale networked groups of prototype nodes with limited operational capability for corporate and government users in different regions of the nation.

d. **Evolving BSX Requirements**

The BSX system is designed to support a number of key requirements that emerge from a systems engineering-based analysis of the needs for
a Black Sky-compatible communication and coordination system. These requirements will be reviewed in detail in later sections.

Key requirements, for example, include:

- **Black Sky hazard protection**: This includes provisions to ensure hardening against cyber, EMP, and IEMI threats.

- **Autonomous network power management**: BSX nodes are being designed to ensure availability of more than 30 days of power through a combination of duty cycle management⁵ and a range of power module configuration options.

- **Autonomous communications backbone**: BSX will not utilize existing, national telecommunications backbone systems.

- **Widely-distributed network**: As a core feature of the system, BSX is being designed for deployment at approximately 200,000 sites within the United States, spanning the locations required to interconnect all infrastructure sectors and their critical supply chains, critical facilities, government agencies, mass-care NGOs, and other key stakeholders to support restoration and sustainment operations.

- **Coordination system hosting**: The BSX nodes and network management system are being designed to host Black Sky-compatible situational awareness framework and infrastructure simulation decision support systems, such as SAND and GINOM.

The architecture, hardware elements, and network management software of the BSX network are all pre-designed to evolve and change. As new information becomes available, including, for example, lessons learned from the catastrophic infrastructure collapse in Puerto Rico following Hurricane Maria, the BSX architecture can continue to evolve.

The core BSX architecture is based on a long-distance radio network (HF/ UHF) for delivery of voice and basic data services. This provides a

---

⁵ The BSX network management system, in combination with continuing GiNOM assessments of projected network usage levels, will make or recommend node-by-node adjustments to power duty cycle (i.e., what fraction of each hour or each day a particular node’s radios will need to be active and drawing power). Power management planning will also be used when nodes are first deployed, taking into account a node’s average expected usage and the expected availability of ~30-day emergency power capability at the deployment site. These factors will be used in making recommendations for the type, configuration, and size of each node’s power module.
pragmatic solution for mission-critical communications requirements in a Black Sky environment. Survivable voice communications will be essential to restoration support and population sustainment operations in Black Sky outages, as will the situational awareness and decision support capabilities the BSX network is being designed to host.

### e. Flexible Communications Device and Data Rate Options

The BSX system design process was based on an extensive trade study. This study examined the suitability of a range of technologies for the unique long duration, stand-alone requirements of the envisioned BSX, and ultimately identified the radio communications system as the best candidate for a nationally-deployed mesh network. The core design provides, even in a relatively sparse network, the voice capabilities and modest data capacity that will be needed in catastrophic scenarios.

In the event of a national emergency, the Federal Communication Commission’s policy is to make additional radio frequencies available (as they have done in the aftermath of the catastrophic 2017 hurricanes in Puerto Rico), thereby increasing the capacity of the baseline BSX configuration. In addition, the Department of Homeland Security can provide designated frequencies for emergency management, which has a similar effect. With the system’s flexible, open, and interoperable architecture, BSX can also include high-density deployments or subnets that can support relatively high data rates in specific regions.

The system is also designed to provide a capability to utilize and interconnect available emergency communications systems. The BSX “smart router-based” design (described below) allows for such additional communications devices to be connected to the BSX system. Those additional devices can be used when available, and compatible with both users’ budgets and needs. Once tied into the system, no actions by the BSX operators are required to select them when they are required to optimize a particular communication path; this selection is entirely automatic.

Examples of such additional communications devices could include:

- High-frequency radios with directional antennas mounted on utility poles
- Mid-frequency radios (including LTE base stations) whose signals are passed via airborne relay units (which are mounted on tethered or free-flying balloons)
Mid-frequency SATCOM services (such as those now used by the Army Blue-Force Tracker)
- Dedicated fiber-optic links; dedicated LTE sub-networks
- Software Defined Radios (SDRs), as confidence in their reliability within large-scale mesh networks grows

**Structure of this Chapter**

This chapter explores the BSX system in detail. Section II provides a brief examination of the communications systems and networks in place today, and an assessment of their adequacy for Black Sky operations.

Section III analyzes the intended users of the BSX system. In particular, following proven systems engineering and design methodologies, this section provides a “social architecture” study for the BSX system. Sometimes referred to as “mission requirements” or “user requirements,” this section specifies four categories of top level user requirements for the system.

**Social Architecture**: Top-level user requirements

1. Who will use the system
2. Under what conditions the system will be used
3. How, and for what purposes, the system will be used
4. The constraints under which that use will occur

Based on that assessment, Section IV uses systems engineering methods to define and assess alternative approaches to the BSX design through “systems engineering trade studies.”

Section V outlines the preliminary design for BSX, with separate subsections for each of the major elements of the proposed system.

Section VI then provides a summary and a set of preliminary conclusions about the BSX system, including recommendations for next steps.
NATURE OF THE CHALLENGE

The current emergency communications landscape consists of an enormous number of stand-alone communications systems. First responders across the nation, for example, currently use over 10,000 disjoint networks for voice communications, with varying capacity for interoperability between them. There are also several additional, dedicated emergency management systems and networks. However, no such system – nor a combination thereof – will be sufficient to coordinate Black Sky sustainment and restoration operations.

---

A. Lessons Learned and Major Challenges

Catastrophes less severe than a Black Sky event have demonstrated both the fragility of the existing commercial communications infrastructure, and the importance of communications during major outages. Hurricane Katrina, for example, was devastating to communications systems, leaving emergency managers “without a reliable network across which they could coordinate.” Emergency plans and communications assets at the local, state, and Federal levels were both insufficient and inadequately integrated for an effective response, verifiably impeding coordination. The command structure of the responders broke down as a result, and communications disruptions “had a debilitating effect on response efforts in the region and the overall national effort.” Indeed, the current lack of survivable electronic communications will undermine critical sustainment and restoration operations in the aftermath of a Black Sky event, intensifying the effects of the resulting catastrophic outages, and could lead to further cascading failures. The effect is cyclical and compounding.

Despite policy changes and greater investment in emergency capabilities prompted by the events of Katrina, a catastrophic event will still cause significant communications infrastructure failures. Significant gaps between

---

8 Ibid.
9 Ibid.
the survivable systems and the capabilities required to navigate Black Sky response operations remain as well.

Hurricane Maria demonstrated the enduring destructive potential of catastrophic events for communications systems, as the storm knocked out nearly all cell sites and internet access in Puerto Rico. The director of DHS’ Office of Emergency Communications testified that first responders were seemingly unable to respond to calls on their own systems, as a result of the damage caused by the storm’s severity. Due to the lack of communications capabilities on the island, intended recipients of relief supplies were unaware of deliveries by emergency managers.

1. Current status and Black Sky capability gaps with deployed emergency communications systems

Some emergency communications systems intended to operate without cellular connectivity remained intact after Maria made landfall. For example, under Emergency Support Function 2 (ESF-2), emergency managers delivered 100 satellite phones to support “essential response personnel supporting communications restoration efforts” in Puerto Rico. However, such an ad-hoc communications system will not be sufficient in particularly catastrophic events, where cross-sector prioritization of critical infrastructure sustainment and restoration will mandate all-sector inter-communication capabilities. In addition to basic functionality issues (e.g., satellite phones do not operate well, if

at all, indoors), inter-communication among many tens of thousands of phones vying for bandwidth would substantially exceed the capabilities of such systems. Moreover, most satellite communications systems cannot operate indefinitely if their ground stations are without power.

a. **Power Limitations**

While Hurricane Maria was not nearly as severe as a true Black Sky event, the response efforts in her aftermath are evidence of remaining gaps in emergency communications capabilities. These gaps could lead to a catastrophic inability to adequately address needs in more severe incidents.

These gaps can also be observed in major earthquake scenarios, which – though they may not always emulate Black Sky events – simulate response operations in some of the most similarly disrupted conditions. Some common themes have emerged in major earthquake exercises.

The extended duration of Black Sky outages will overwhelm backup and emergency communications capabilities. While participants in the 2011 National Level Exercise (NLE-11) had some success establishing emergency communications channels, for example, their success was measured over a theoretical 48-72 hours. The NLE-11 AAR found that, in a more-extended outage, communications infrastructure would steadily degrade as emergency assets ran out of generator fuel.15 The Cascadia Rising exercise, simulating a 9.0 earthquake and subsequent tsunami in the Pacific Northwest, also found that emergency managers and coordination centers are ultimately

“not prepared to operate in a degraded communications environment over an extended period.”\textsuperscript{16}

b. \textbf{Interoperability Shortfalls}

Interoperability between current public and private systems is another key impediment to successful coordination in Black Sky outages. As the previous chapter noted extensively, infrastructure owners and operators will need significant, ongoing communications with government emergency management personnel at multiple jurisdictional levels. Doing so, however, has proven to be a challenge. Private sector participants in the 2014 CAPSTONE-14 earthquake exercise, for example, found that requesting resources and sharing information with the State EOC was “nearly impossible” due to a lack of interoperability between the government and private emergency communications systems.\textsuperscript{17}

All-sector, public-private interoperability will be a key requirement for a Black Sky emergency communications system. Given the repeatedly-experienced difficulty of achieving a truly useful level of interoperability between differing communications systems, having all sets of actors interlinked into the same system would be the most effective way to achieve this wide interoperability.


Due to the nature of many leading government emergency communications capabilities and infrastructure, however, this is not currently possible. The National Guard’s Disaster Incident Response Emergency Communications Terminal (DIRECT), for example, links National Guard forces, first responders, emergency managers and state and Federal authorities.\(^{18}\) Notably absent, however, are the utility owners and operators who will be at the forefront of response operations.

Similarly, FEMA’s Mobile Emergency Response Support (MERS) vehicles, which can provide response officials with a combination of communications capabilities\(^{19}\), do not include interoperability with the utility owners and operators that will have primary responsibility for sustaining and restoring critical infrastructure in Black Sky events. Successfully coordinating Black Sky response operations will require a single system that can interconnect all relevant sets of users.

c. **Black Sky Hazard Hardening**

Emergency communications systems must also be resilient against adversary efforts to undermine them. Attacks on critical infrastructure are likely to involve cyber and/or physical attacks on communications systems, given the criticality of the capabilities they afford to incident response efforts. Indeed, the Federal Communications Commission (FCC) acknowledges cyber threats as “perhaps the largest vulnerability … of the national communications infrastructure.”\(^{20}\)

All parties involved in sustainment and restoration operations in the aftermath of a Black Sky event may face the additional threat of electronic jamming technologies. Jamming can impair GPS, radio, and other wireless systems, threatening situational awareness and coordination efforts.\(^{21}\)

---


DHS is only beginning to examine anti-jamming techniques and tools to lessen the likelihood that their communications in a catastrophe will be obstructed or delayed.

B. Incorporating Current Systems

Despite the shortfalls of current systems, government departments and agencies are unlikely to abandon them outright. The BSX system has therefore been designed with the ability to incorporate them, along with significant interoperability planning and testing, to ensure existing capabilities can interconnect. BSX would also benefit from including relevant government stakeholders in system development and implementation to catalyze this process. For radio-based legacy emergency communications systems, integration should be relatively simple, as such interoperability is already being incorporated into the BSX design.

Some organizations may plan to depend on less-survivable systems. To address the risk of loss of internal communications when such systems predictably fail, such organizations could deploy additional BSX nodes, which include an embedded LTE base station that can provide local tie-in capabilities for cellphone users.

The BSX design calls for deployment to ultimately span all key infrastructure sectors and supply chain entities, as well as government agencies and other critical facilities and stakeholders. In total, our system analysis estimates that
deployment of approximately 200,000 nodes will be needed across the United States (see figure XX, above). Any locally-provided emergency communications equipment that already exist at these sites can be retained and interconnected to the BSX system, to provide additional capability.

The National Public Safety Broadband Network (NPSBN) has significant potential value in terms of complementing the envisioned BSX system. The NPSBN – which AT&T won a contract to build in March 2017 – will be a “nationwide wireless broadband network dedicated to America’s first responders,” intended for both day-to-day use and disaster response operations.\textsuperscript{22}

However, in addition to deployment limitations (i.e., only to first responders and certain pre-selected additional facilities),\textsuperscript{23} NPSBN is overlaid on top of the existing AT&T cellular network. This network will not continue to operate for the long durations required to address a subcontinent-scale power outage, nor is it specified to survive Black Sky hazards such as EMP or sophisticated cyberattacks. Nevertheless, this data transmission-focused system could play an important role in supplementing an all-sector deployed BSX network during the brief period when the cell networks may be available, immediately following a Black Sky event.

However, such complementarity must be planned before a Black Sky hazard strikes; it cannot be improvised after the onset of such an event. By transferring lessons-learned from the BSX design to that of the NPSBN, pre-planning may also help ensure that NPSBN infrastructure will be more resilient against Black Sky hazards, have access to some of BSX’s emergency power capabilities, and potentially be tied in to the all-sector connectivity planned


\textsuperscript{23} Ibid.
for BSX. Given that the NPSBN is still in development, a valuable time window exists to add these features and overall interoperability in the design stage, rather than tacked on as an addition at the end of its development.

C. Emergency Communications Policy

Those primarily privately-owned segments of critical infrastructure sectors that will need to survive in Black Sky scenarios will generally require the widest deployment of (and have most urgent need for) BSX nodes. Nevertheless, local, state, and Federal government agencies will also need to be tied into such a system to ensure they will be able to effectively communicate, maintain adequate situational awareness, and benefit from the hosted decision support system.

The Federal government should also consider improving emergency communications-related policy. The current primary document, the 2014 National Emergency Communications Plan (NECP), does not sufficiently consider the primary role industry will play in critical infrastructure sustainment and restoration following Black Sky events, and therefore their level of involvement in emergency communications. Indeed, the NECP states that ‘Communications for Incident Response and Coordination’ are “primarily government-to-government functions…”

This, however, will not be the case in Black Sky scenarios, or even in more extreme gray sky situations. As became clear in Puerto Rico, without pre-

Utilizing BSX and its hosted situational awareness and coordination capabilities to help Federal agencies meet legislative and policy requirements could offer special benefits, especially for Black Sky attacks on the grid tailored to jeopardize U.S. national security.

planned Black Sky-compatible resilience investment and operational multi-sector coordination, all sectors will collapse. Electricity, food, fuel, water, finance, health care, pharmaceuticals, transportation, security, and all other sectors, primarily made up of corporate suppliers, will be the main focus for infrastructure restoration and population sustainment following a Black Sky event.

The NECP also largely provides strategic, rather than operational, direction for the emergency response community. The detailed, pre-event coordination and operational planning required to successfully navigate Black Sky events will therefore likely need to be addressed in a separate (but complementary) effort. This operational guidance should, however, be developed in tandem with BSX or a comparable platform.

In addition to the NECP, Executive Order 13618 (Assignment of National Security and Emergency Preparedness Communications Functions) guides high-level emergency communications planning. EO 13618 codified specific requirements for relevant Federal departments, officials, and committees, as well as testing and reporting requirements, and created a National Security and Emergency Preparedness Communications Executive Committee co-chaired by DHS and DOD. Enabling the BSX initiative to help Federal agencies meet these requirements could offer special benefits in Black Sky events, especially those involving attacks on the grid that are tailored to jeopardize U.S. national security.

---
The first step in designing a system that can fill the gaps in existing emergency communications and coordination systems lies in developing a “social architecture” for the BSX. This social architecture identifies the users and customers for BSX, determines how they define value within their operational context and, in general, captures the information necessary to create a system that is both effective and suitable for their mission.²⁶

²⁶ “Effective and suitable” is the terminology used in the U.S. Federal Acquisition Regulations, or FAR. See “Federal Acquisition Regulation (FAR),” General Services Administration, last updated January 19, 2017, https://www.acquisition.gov/?q=browsfar.
A. Anticipated BSX Users

The social architecture starts with the question of “who?” – i.e., who will be using this system? Specific details about the intended users are also critical. What are their objectives? What are their needs? What are their skills? What constraints are imposed upon them?

The recommendations in Chapter I provide the starting point for establishing the system’s user base. Critical personnel from the public and private organizations described in the previous chapter’s revamped disaster response architecture will all be key users of the BSX network. However, the full scope of organizations that will need to be tied into this system must replicate, at a carefully defined, reduced level, the full range of organizations involved in the production, distribution, marketing, and management of all the resources and services needed to sustain millions of affected people, and to restore, supply and resupply all essential infrastructures.

- **Government Users: Federal, State, Local, Tribal, and Territorial**
  For the Federal government, users would include: the National Response Coordination Center (NRCC); ESF Coordinators and Sector-Specific Agency leadership; the organizations in operational support roles such as the National Infrastructure Coordinating Center, the National Operations Center, Office of Cyber and Infrastructure Analysis, National Business Emergency Operations Center and Joint Field Offices; and key White House personnel. It will also be critical to include state, local, tribal, and territorial (SLTT) leaders and
emergency managers, as recommended by the National Emergency Management Association.²⁷

- **Regional Reliability Administrators: An Expanded Role**
  Consistent with the realigned structure of FEMA as proposed in Chapter I, regional Reliability Administrators (RAs) would take on an expanded role in Black Sky response operations. These RAs will provide coordination guidance in support of infrastructure sustainment and restoration in each FEMA region and be trained to use the BSX system in disaster operations. In particular, the RAs would utilize the BSX-hosted coordination capabilities, including the situational awareness and decision support functions, to help prioritize and manage infrastructure operations throughout all phases of an event. These teams would also benefit from participation in cross-sector exercises that utilize BSX nodes, or simulations of such nodes.

- **Mass Care NGOs**
  Mass care NGOs will have a particularly vital need for the BSX system. Their services will be very much in demand in complex catastrophes of this scale, and the wide-ranging support roles they will need to play will only be possible if they are fully linked into a Black Sky-compatible communication and coordination system.

- **Private Sector Users**
  In the private sector, essential users will include Cross-Sector Coordinating Council (CSCC) leadership, as well as operations

personnel from corporations and other organizations in all critical infrastructure sectors (e.g., electric power, water treatment, water pumping, sewage treatment, natural gas main-line operation, food, health care, and security, transportation) who will be carrying out prioritized sustainment and restoration operations.

Corporations involved in the production, storage, and distribution of resources and services in carefully-defined segments of critical supply chains will also be essential in Black Sky scenarios, and will need to be included as BSX users.

As the BSX system’s deployment evolves, BSX training will become an important addition to training programs in user organizations. It will also be essential to include key managers in cross-sector exercises which utilize either BSX or a simulated version of the system.

B. Phasing of Sustainment and Restoration Operations: Implications for BSX Design

Based on this wide range of users, this study identifies primary examples of “use-cases” for BSX in support of restoration, sustainment, and emergency response operations.

1. BSX Use-Cases

Overall, the system must provide voice and (limited) data communications to assign, coordinate, and perform actions required for ongoing service sustainment and restoration operations.

- **Cross-Sector Communications for all Infrastructure, Resource, and Service Suppliers:** Provide cross-sector voice communications capabilities to coordinate essential restoration operations and address interdependent, cross-sector support requirements. This would include: communication among many cranking path sites, including corporations providing loads for black start operations; the delivery of water to electric facilities; prioritized power restoration for water
facilities; food and pharmaceutical distributors to support restoration teams and their families, etc.

- **Situational Awareness Data Gathering**: Support both automated and manual forms of situational awareness data gathering for use by the BSX-hosted SAND™ system.

- **Private Sector – Government Coordination**: Provide for voice and modest data communications between infrastructure, resource supplier, NGO, and service sector users with local, tribal, state and Federal agencies.

- **Family Communication**: Provide communications between employees at work and their families, perhaps indirectly through an intermediary such as the Red Cross or other NGOs.

- **Transportation**: Support the coordination of emergency response operation logistics and supply actions across multiple sectors, e.g., communicating with those who are moving or allocating scarce resources and/or personnel.

- **Cross-Sector Coordination Organizations**: Support the operations of corporate and government cross-sector coordination bodies, such as those described in Chapter I.

2. **Sustainment and Restoration Operations Phases**

The following overview of sustainment and restoration “phases” provides a framework which can be helpful in identifying different requirements for an emergency communications system. In practice, many or perhaps most of these phases would overlap, and each phase would encompass far more complex interaction with other sectors than that summarized below.

a. **Phase I: Alert and Protective Measures**

Sustainment and restoration operations will proceed in stages. The first stage consists of a two-part process. Initially, all personnel will need to be alerted that the event will require Black Sky protocol to activate the associated teams and initiate appropriate, predefined actions. This very early stage may, in part, be accomplished with normal telecommunications systems during the first minutes and hours after a Black Sky event, if they are still functional during that period.
The second stage of Phase I will be the adoption of protective measures, in which utility, resource, and service supplier personnel will take configuration actions that protect equipment against further damage. Emergency personnel will use BSX communications capabilities to provide status updates to key decision makers in all sectors, including power grid Reliability Coordinators, FEMA Regional Administrators, and officials in Joint Field Offices, allowing them to understand the configuration of key infrastructure assets.

Critical infrastructure service providers and supply chain companies will have a designated emergency manager using the BSX system to coordinate their efforts with regional coordinators and relevant managers in all other sectors. In turn, such managers will work with their peers in other sectors and regions, with state and Federal emergency managers, and with other relevant response stakeholders.

b. Phase II: Status Assessment and Repair

The next phase is the status assessment and repair. In this phase, response teams determine the location, severity, and system impact of specific infrastructure damage; share status updates; and work both within their organization and with others, as required, to implement necessary repairs, replacements, or workarounds for damage. For infrastructure and resource suppliers that must sustain limited operation, this phase will take place in parallel with the initial “protection” phase.

c. Phase III: Restoration / Ongoing Sustainment Operations

This phase will differ significantly for infrastructure, resource, and/or service suppliers involved in restoring systems that have shut down, vs. those that are working to sustain limited operation.

- Restoration

For entities involved in restoration, the electric subsector provides a primary example:

Electric company operators, initially, will need to reach out over the BSX system to security organizations and local and state institutions that can help secure roadways to ensure both essential personnel and critical assets can be transported to key work sites. Efforts in this phase will also typically include communication with suppliers of
those key assets, including diesel fuel for black start generators, food and pharmaceutical supplies for workers, coordination calls with mass care organizations to ensure adequate shelter is available for families of key workers, etc.

Following this step, company operators will use the BSX network to facilitate internal operations and work with other power companies and facilities that will receive power (“load” companies) to coordinate manual black start operations. Each stage in this effort will involve extensive voice communications among the many teams and facilities along a black start cranking path.

Operators will use the BSX system continuously during this process to synchronize actions: e.g., setting relays, starting generators, and configuring the designated electric loads. This process is complex and communication-intensive, typically involving hundreds of switching operations spanning the many facilities of even the simplest black start cranking path.

As the process takes place, operations teams will likely also use the BSX system to request replacement parts, request the loan of specialized personnel, call for requisite consumables (along with transportation and security support), and provide status reports and predicted recovery timelines to decision makers at higher levels in multiple sectors.

Conceptually, initial power restoration may be visualized as concentrating on restoring “islands” of relatively small service areas, implemented via direct links from generation stations to major, critical users of electric power. For this phase, voice communications and

The electric subsector will have an intensive need for basic, widely connected communications. The manual black start process will involve verbal coordination of multiple teams distributed along a “cranking path.” Such widely connected systems will also be vital for resupplying critical consumables, as well as transportation and security support for electric subsector restoration operations.
modest data (e.g., photos of key equipment configurations) will be the primary need.

As information about the status of power lines and substations is accumulated, corporate operations managers can communicate over the BSX network with their counterparts in other regions – if national telecommunications “back haul” systems are not yet restored – to re-establish “island-to-island” interconnections. Electric utility operators will transition the restoration from a set of discrete islands back towards the “power grid” of nominal operations. This will allow restoration of power to customers that may not have been included in the islands. There may not be electricity provided to residences and businesses during the initial “islanding” phase of recovery operations, as priority will be placed on restoring power, for example, to natural gas pipelines, water and wastewater plants, and other critical facilities. As summarized above, while this section (and the associated figure) focused on electric subsector restoration as an example, BSX is designed to support, in a similar way, restoration of all relevant sectors.

- **Ongoing Sustainment Operations**

It will be essential for most critical sectors to continue the production and distribution of at least some minimal resources or services during long duration power outages. This will include, for example, continued (though reduced) operation of water and wastewater plants, critical subsets of food and pharmaceutical production and distribution, operation of critical military and security facilities, and many others, likely relying on emergency power generation. This continued operation will rely extensively on cross-sector support, and, therefore, on the BSX system for coordination.

Most infrastructure sectors will primarily be working to sustain production and distribution of critical products and services. This will involve a particularly complex use of the BSX system, since all production and distribution involves supplies and support arising from many different sectors.
For this scenario, the water sector may be used as a primary example. As soon as a water company becomes aware that a power outage is expected to continue for a long duration, operations managers will need to implement Black Sky protocols for their systems. For a megacity, for example, this might mean resetting control valves and instrumentation to minimize system pressure; shutting down service to higher-altitude regions of a community that require power-intensive water system pumps (“lifts”); and taking steps to reduce water treatment to pre-arranged minimal levels that can provide potable water, while minimizing the need for replacement of diesel fuel for emergency generators and the need for chemical consumables. That initial step will require extensive communication within a water company, as well as coordination with relevant government agencies. However, once Black Sky protocols are implemented, communications needs will change. While there will be an ongoing need for communication with support teams at different locations in the field, there will now be an urgent need for cross-sector communication to ensure government emergency response personnel are working to bring in replacement fuel and treatment chemicals before existing stocks are exhausted. And, as in the previous example, throughout this process, water system operators will also be reaching out to other sectors to acquire transportation and security support, as well as food and shelter for sustainment teams and their families.

While the restoration and sustainment operations outlined above are proceeding, emergency managers at all levels of government and across all industry sectors will be in regular communication, reviewing the situational awareness information provided by the SAND system, and jointly considering prioritized actions recommended by GINOM (where the time-sensitivity of an action permits such discussion). These decision makers would be coordinating closely with mass care NGOs and supporting other emergency response efforts, including security, fire suppression, and transportation teams – both internal and external to their organization – through the BSX nodes deployed within those organizations. At the same time, they may also use BSX, as required, to communicate with senior political decision makers at all jurisdictional levels.
Enabling this process requires continued availability of key consumables and other goods and services from supply chain providers. These providers will need to be “Black Sky-certified” to ensure that they have the ability to operate in extended outages. In addition, such Black Sky-certified organizations will need BSX nodes which enable them to communicate with emergency management agencies and key operations managers in the corporations they supply. The need for such supplies, given their extremely limited availability in Black Sky outages, will be a key focus of GINOM’s AI-enhanced decision support capability, hosted by the BSX network. In complex catastrophes of this magnitude, the need for such “machine assistance” is amply supported by research and analysis of less severe scenarios.\(^\text{28}\)

C. BSX User Requirements:
Social Architecture Analysis

In developing the social architecture or “user requirements,” the BSX team consulted with domain knowledge experts in different sectors, including operations managers of utility sectors. High-level conclusions from this process are summarized below.

1. Social Architecture: User Requirements for BSX

   a. Set up time and labor

   BSX should be designed so that a single trained operator can set up the emergency communications suite at a designated location (i.e., implement

the transition from the long-term storage configuration into the operating configuration) in 4 hours or less.

This limitation on setup time and labor requirements drove the down-selection process on how the emergency communications equipment is configured for long-term storage, the portability of system modules, the complexity of integration and alignment requirements, and a range of other, subsidiary criteria.

b. High reliability

BSX should be designed so that – unless there has been physical damage sustained at a particular node – 99% of the locations should be able to operate (in at least a partial capacity) after being brought out of long-term storage. Achieving this level of reliability and availability will require some pre-deployment of selected spare parts at every site.

c. Automated network establishment

The emergency communications system should be designed so that if at least 90% of the nodes in a region are brought into operation, along with at least 75% of the nodes in adjacent regions, then at least 75% of the emergency communications system nodes within that region should automatically discover a route to designated key system hubs and decision makers (Joint Field Offices, key coordination facilities in critical sectors, etc.).

Additional nodes can achieve connectivity to the local emergency communications system hub through manual operator actions. Achieving this high level of reliability and connectivity will require the use of multiple data paths for most of the point-to-point linkages needed by users. This in turn implies a need for multiple communications devices of different types at most node sites.

d. Voice and limited data connectivity, and prioritization

Push-to-talk voice communication (both one-person-to-one-person and “conference calling”) serves a high portion of the emergency

---

29 Connectivity, in this context, means “achieve at least push-to-talk voice and a modest data” capability.
communications system use-cases encountered in the research that defined the baseline, core system configuration. The next-most-important capability is the ability to send digital photographs between nodes. More generalized data service is a still-lower priority. These priorities will be used to establish dynamic priority-of-service within the emergency communications system.

As indicated earlier in this chapter, higher data rate options can be provided as required, regionally, by system users, by investing in additional dedicated nodes that support such data rates.

e. **Power requirement optimization goal**

As indicated above, when the BSX system reaches full deployment, the BSX social architecture analysis identified the need for approximately 200,000 system nodes across the United States. Cost per site is therefore a design consideration. Initial cost sensitivity assessments suggest that the 30 to 60-day power requirement is a significant contributor to the cost of a fully deployed system. As the technical design evolves through multiple “block” deployments, this represents an area that will require careful optimization with each user and user community to reduce the power requirements and make case-by-case implementation decisions that minimize cost without decreasing operational availability.

f. **Hosting situational awareness**

Although extensive pre-event planning will be required for Black Sky scenarios, no plan will survive the first hour of an actual event without requiring extensive modification. A design compatible with hosting a capability like the Situational Awareness Network Diagnostic (SAND™) system, which provides evolving, real-time situational awareness is therefore essential. Decision makers in all sectors will use this information to adapt plans to the actual situation on the ground, and to communicate the altered plan to those in the field.

g. **Hosting multi-sector modeling and simulation for decision support**

Despite the criticality of real-time situational awareness for decision making, the scale of infrastructure and resource sustainment and restoration requirements will far exceed the capabilities of operators and decision makers without machine assistance. As a single, interoperable,
widely deployed, multi-sector system with provisions for long-duration power and hosted situational awareness capabilities, BSX is also an ideal host for a simulation model that can provide interdependency mapping and AI-enabled decision support in Black Sky scenarios, such as the Global Infrastructure Network Optimization Model (GINOM™). The BSX network, computer resources, and user interface are therefore designed to support such a simulation engine.

h. Multi-sector deployment scale

In a Black Sky outage, response operations – including the prioritized sustainment and restoration of critical infrastructure, resource, and service suppliers and their tiered supply chains, as well as population sustainment – will require significant planning, and eventual “Black Sky protocol” certification for a complex web of stakeholders. This may include corporations, government offices, and NGOs spanning the most important public and private sectors. Since communication across this full range of organizations will be essential, BSX nodes or node clusters will need to evolve to include deployment with selected, regionally-distributed organizations in all such public and private sectors. The current estimate for the ultimate scale of BSX deployment across the United States is greater than 200,000 nodes, and the scale of deployment necessary is likely to expand over time. The BSX system and network’s architecture is designed to be compatible with further scaling, as required.

i. Multi-sector deployment socialization

BSX may be compared, metaphorically, to a nervous system. In this case, it is the “emergency nervous system,” activated in Black Sky conditions to replace the normative telecommunications / internet nervous system of the organically interconnected infrastructure sectors and resource and service suppliers that support our modern world. Thus, a critical requirement for the viability of such an emergency communications system is wide, multi-sector deployment. Moreover, nearly all contemporary supply chains are international. Although initial BSX deployment will be focused on encouraging development of a sparse network across the United States, ultimately, deployment of an emergency communication and coordination system that can serve this need – either BSX or some compatible, comparable system – will be needed internationally.
Successful BSX deployment mandates an expanding socialization process that can successfully reach out across nearly all public and private sectors in the U.S. and, eventually, in partner nations. Given EIS Council’s mission to host multi-sector, coordinated planning for Black Sky events, the organization, at all levels, is committed to using its unique cross-sector and international presence and connectivity to help drive this socialization process.
Following the framework of user requirements or “social architecture” summarized above, the next step in system design was to map the associated requirements and goals to candidate solutions in a series of systems engineering trade studies. This process was undertaken through several steps:

- Identifying candidate communications technologies
- Developing a list of key issues and risk areas
- From that list, identifying a set of associated technical trade studies
- Developing candidate designs, together with methods and metrics for selecting among those candidate designs
- Using those methodology and metrics, making the initial design selection, along with an assessment of the feasibility and performance of the selected design.
This five-step process is summarized in the corresponding sections, below.

2. **Candidate Communications Technologies**

The BSX development team identified an array of communications technologies as initial BSX candidates based on the team’s systems engineering analysis and experience in implementing a variety of high-reliability communications systems\(^\text{30}\). These candidates included:

- Network-supported HF radio
- Network-supported UHF radio
- Network-supported VHF radio
- Network-supported higher-frequency radio
- Network-supported meteor-burst radios
- Use of power lines to carry communications signals
- Dark fiber communications cables\(^\text{31}\)
- Commercial satellites (low-Earth orbit)
- Commercial satellites (geo-stationary orbit)
- Various combinations of the above

3. **Key Issues and Risk Areas**

Given the results of the social architecture and the above list of candidate technologies, the BSX development team identified a number of key risks to be addressed through the technical trade study process. Through that process, a condensed list of issues and risk areas were identified, summarized below, representing a combination of likelihood and potential impact that made them possible key system disablers if not properly addressed and mitigated.

**Issues and risk area summary**

a. How to provide power for the emergency communications system at each location for the specified 30 to 60-day period?

---


\(^{31}\) Fiber optic communications cables that are installed but not in active service.
b. What spectrum (RF frequencies) would be available for the emergency communications system during emergency operations? Not all of this spectrum allocation need be available for use during nominal (non-emergency) use.

c. What techniques and materials would allow the emergency communications system equipment to be stored for long periods of time (years or decades), yet still be periodically tested, maintained, and support periodic training?

d. How to allow the emergency communication and coordination system to adapt, ideally almost automatically, to the likely differences between the anticipated emergency conditions and those that actually come to pass?

4. Technical Trade Studies

Given the above list of significant risk areas, the BSX development team identified key trade studies that would be required.

- How to provide 30-day self-contained power with a long storage life, reasonable maintenance requirements, and high availability at need.

- Assess spectrum availability during emergencies and, based on that assessment, select the actual communications mechanisms (and eventually the actual devices) for the core network. Also required is the selection of an enabling network design that will permit smooth evolution to incorporate new technologies and devices as they become available with adequate, demonstrated reliability.

- Determine the approaches and materials required to achieve effective long-term storage of the emergency communications system equipment.

- Identify techniques to support self-adaptation of the emergency communications system.

The results of these trade studies led to a candidate solution, presented below, which also permitted reasonable technical approaches to mitigate all risk areas. Though there was no explicit “design-to” per-site cost, the selected approaches, at top level, were assessed to allow cost effective implementation options.

One area that will require coordinated optimization between user and supplier will be selecting optimum, specific implementation of the “30 to 60-
day power” capability appropriate for the needs of different users and sites. Where nodes cannot depend primarily on facility-provided emergency power, the specific mix of technologies selected will vary from site to site. Selections for each site will be made from a range of options, depending on specific user and site requirements.
This section describes the candidate design, along with the trade studies that validated the efficacy of that design.

The systems engineering process, described above, allowed the BSX development team to select an optimum overall network architecture, along with key technical parameters (such as radio frequencies and transmission polarizations for the system’s core network). More detailed parameters will be selected during detailed design of each anticipated deployment block (e.g., exact RF power levels, antenna sizes, and manufacturers).

Finally, this section assesses the technical feasibility of the proposed design and estimates key system parameters such as availability, network connectivity rates, and storage life.
A. Top-Level Summary of the Selected BSX Design Solution

Resulting from a review of the identified user requirements and analysis of the full array of key concerns and issues, a subset of key requirements were identified as design drivers:

**BSX System Design Drivers**

- The BSX network and nodes must survive the onset of a Black Sky event, no matter which of the identified hazards caused the event.32
- All nodes must operate for 30 to 60 days without grid-provided power.
- The BSX network must support deployment of at least 200,000 sites (“nodes”) across the United States, and appropriately-scaled system deployments in other countries over time.
- BSX must provide the capabilities needed to support sustainment and restoration operations in complex catastrophes. This includes hosting situational awareness and decision support systems, for use by a hierarchy of users distributed across all infrastructure, resource, and/or service supply sectors, and their government and NGO partners.

---

32 For a detailed assessment of broadly accepted hazards that could take place at the Black Sky level, see “Black Sky Hazards,” EIS Council, n.d.a., http://www.eiscouncil.com/BlackSky.
Figure E depicts the elements of the selected BSX design solution. As the figure shows, the selected BSX system architecture may be summarized as four interactive elements and capabilities.

**BSX System Elements and Capabilities**

- Black Sky hazard survivable communications devices.
- Black Sky hazard survivable emergency power (i.e., designed to survive the actual Black Sky event, and capable of operating for many weeks), either self-contained or available from the facility where deployed.
- Hosting capability for situational awareness and multi-sector modeling for decision support.
- Features that provide physical, cyber, and EMP protection to the BSX system. These will be necessary both during the long period while it is being stored, prior to the onset of a Black Sky event (potentially decades at unmanned locations), and during and after the event, as the BSX system is being used to implement sustainment and restoration efforts.

Consistent with the design drivers and the resulting, selected approaches reviewed above, specific components were selected as primary elements of the core Black Sky-survivable BSX communications subsystem.
Core devices at each BSX node location

- HF NVIS radios, with small magnetic antennas
- UHF radios
- Packet routers equipped with special, mission-specific software agents
- Network management software to implement and control the above functions
- A power module, baselined to utilize vanadium redox flow batteries, with control circuitry to enhance reliability, supplemented at many locations by solar panels. The system must be compatible with alternative power supply options, as well as alternatives to solar panels for supplemental power (e.g., wind-powered generators).

Regional coordination centers and other, selected, node clusters will also include:

- An “intelligent director;” A packet router equipped with additional special, mission-specific software agents.

The emergency communications system may optionally include the following components:

- Mobile emergency communications system nodes (e.g., trucks or other vehicles that are equipped with emergency communications equipment, a packet router, and appropriate power equipment).
- Other enhancement features, where required, such as an NTE base-station to permit tie-in of local cell phones at short ranges.
- Mobile emergency power modules, which can also be used to power other types of equipment, if needed.
- Tethered drone nodes to enable longer distance use of UHF devices, especially where judged helpful due to unique requirements, terrain, or atmospheric transmission issues.
- Additional devices dedicated to higher bandwidth communication, where required, typically in special, higher node-density regions.
B. Network and System Design

The devices summarized above will be linked in a mesh network, capable of scaling beyond hundreds of thousands of nodes or node clusters.

1. Network and System Design Characteristics

a. Site to site communications

BSX will leverage the strengths of HF and UHF radios to provide site-to-site communications. UHF provides very high-quality service, but at a shorter range than HF. HF radios, however, can operate beyond line-of-sight. Both frequencies are therefore included. The disadvantage of large size traditionally associated with HF radio antennas is corrected through the use of magnetic antennas.

b. Power module

If on-site emergency power is not available, nodes will provide stand-alone power for 30-60 days. Power module sizing will be based on projected requirements of the radios’ duty cycle for each node. The size of stand-alone power modules, where required, will therefore vary from site to site. In such cases, BSX software will manage the site’s power consumption based on input from GINOM regarding projected use timelines for a given node.

Users will also select from a range of power module configurations. At many sites, the size and cost of the power module may be decreased by the addition of solar panels or, where suitable, wind power or other approaches.

c. Mobile nodes

Vehicle-mounted emergency communications system configurations will be important for many user categories. The UHF component could be configured to operate on-the-move, though the HF NVIS component will likely be configured only to operate at-the-pause (i.e., when the vehicle is parked). Power for the emergency communications system equipment on these vehicles will be provided by a combination of batteries and enhanced vehicle alternators.
d. **Accessory, portable power modules**

For nodes that require power modules, a range of configuration options could provide for long duration power storage, including a battery technology that allows storage, fully charged, for many years. Battery-based power storage provides a unique advantage for urgent, high-criticality equipment or facilities that may experience a sudden power outage extending beyond the capability of their emergency generator(s) and/or available fuel reserves. Users may therefore wish to have accessory BSX modules available for use in such unforeseen events, providing them with a portable power source that can be moved from site to site during an emergency. These accessory modules could also function as spares for a user’s BSX node cluster.

e. **Communications protocols**

The single-hop, direct site-to-site communications success-rate is improved through the use of error correction coding, and other higher-level communications protocols. These are implemented in the packet router located at each emergency communications system site.

f. **Automated, optimized radio selection**

There are two independent radios on different frequency bands at each site, utilizing different modulations. This provides a basic type of communications path diversity, and thereby improves system reliability. The router at each site determines which radio to use for each transmission attempt (whether voice or data) based on its radio “visibility” to adjoining sites. No manual action is required by the emergency communications system user to select the best radio for each transmission, as this is accomplished for them automatically. Emergency personnel will not be required to have RF propagation expertise.

g. **Automatic multi-hop path selection**

The packet router also uses the same visibility information to implement multi-hop communications for both voice and data. A communications link need not be “direct,” meaning the data may be routed through other emergency communications system sites as intermediate nodes. The finding and utilization of such paths is automatically accomplished by the
packet routers. No manual action is required by the emergency personnel to find and implement such multi-hop paths.

h. Interoperability with non-BSX devices or networks

BSX will link in and use other existing communications systems if they are available. If a local organization (e.g., utility) has provisioned an emergency communications system for their own facilities, that system can be linked into the BSX network by connecting it to the packet router at a BSX site and incorporating a special “bridging” software agent at that router.

This capability allows the BSX network to interconnect any available emergency communications systems as subnets, which then have availability to interconnect with all other nodes on the BSX system.

i. Frequency selection

Frequency selection is based on time-of-day, atmospheric conditions and other factors. An “intelligent director” (a packet router equipped with mission-specific software agents) controls and coordinates this process, providing direction to the packet routers, which in turn command the radios to use the appropriate frequencies and other radio settings. No manual action is required by emergency personnel to account for day/night frequency preferences or other, related frequency selection factors.

The overall policy for frequency utilization must be coordinated with regional and national civil officials. This coordination, however, is also implemented in the intelligent director; no manual action is required by emergency personnel to comply with ever-changing radio-frequency policies.

j. Hosting Situational Awareness and Decision Support

Coordinating bodies and decision makers in all sectors will be tasked with manually “replicating” at least minimal portions of the self-sustaining infrastructure and resource supply networks that, under ordinary conditions, deliver all products and services used in modern societies. However, they will be tasked to do so in a highly disrupted environment. This will not be possible without extensive, multi-sector situational awareness information, available, in a digestible format, to most decision
makers. The SAND™ system, referenced above, provides an example of such a capability.

Even with such situational awareness, however, the sheer number of decisions required, and the vast array of data that will need to be “manually” monitored, will greatly exceed capabilities of human operators without machine assistance. In a Black Sky event, industry and government personnel conducting infrastructure sustainment and restoration operations, or addressing the needs for population sustainment, will require a model which includes both interdependency mapping and an AI-enabled simulation, as well as a forecasting engine that could provide decision support functionality. The GINOM™ initiative, referenced above, is an example of this two-level capability.

Since BSX is envisaged as an interlinking system that connects to all such sectors, designed to survive and operate in Black Sky scenarios, the system is ideally placed to host both of these capabilities.

2. Design Validation

The next step in the systems engineering process is to validate the overall design outlined above.

To do this, the BSX team developed a performance model using inputs based on sample product specifications (for key elements of the system design) and on the overall system requirements and goals summarized above.

Figure F depicts the methodology used to implement this process, providing a preliminary validation of some of the key technologies selected for the survivable communications element.

A system performance model makes various assumptions about certain aspects of the system it is modeling. Drawing upon actual performance achieved by similar systems to refine these assumptions is essential for creating a high-credibility model. This was a key consideration in BSX model development. Dr. Neil Siegel, for example, the principal author of this chapter, was a key part of the development team. Dr. Siegel was also the program manager for the U.S. Army “Blue-Force Tracker.” This Army system uses VHF and UHF radios interconnected via local routers to implement its communications network, similar in some critical ways to the communications systems selected for

---

33 Formally known as “Force XXI Battle Command Brigade-and-Below”, or FBCB2.
BSX. The Army system was fielded in 1999, and has been in successful and continuous operational use since that time.

Dr. Siegel, working in partnership with Bran Ferren, co-founder of Applied Minds LLC, has deployed and successfully used similar emergency communications systems in a variety of locations worldwide. The emergency communications system which, uniquely, operated successfully during the Superstorm Sandy blackout represents one of many examples of their joint efforts. By working together in support of EIS Council’s BSX development, Neil Siegel and Bran Ferren were able to apply lessons learned from several relevant projects, and thereby ensure that the BSX design leverages this full range of experience. Many of the key features selected for BSX have been validated through their use in these prior systems.

The motivation for the design of the above-mentioned Army system, in particular, was similar to that which underlies the goals for BSX. Requirements included very high levels of reliability, and the design solution was to achieve this via communications path diversity – multiple radios, on different frequencies, using different waveforms, with the best path determined in real-time by the attached routers.

---


In one cardinal way, the Army system was much more difficult than the BSX: most of its nodes must operate while on the move, and therefore had to deal with continuously-changing line-of-sight interruptions, interruptions caused by terrain masking and foliage masking, and other related issues. Most of the operating locations for BSX are, in contrast, at fixed sites and do not face these difficulties. On the other hand, the envisioned BSX sites are on average farther apart than the units for the Army system. This led the BSX team to select HF radios as a key element of the core architecture used within BSX nodes, as HF can achieve longer single-hop communications distances than the VHF and UHF radios used in the Army system.

Key elements and capabilities of a BSX prototype were successfully demonstrated in a subscale field test as part of the EPRO SECTOR Executive Committee Meeting, Winter 2017. This demonstration took place on December 12, 2017, at PJM Interconnection headquarters in Audubon, Pennsylvania.

As noted at the bottom of Figure F and shown in the image below, the BSX team successfully conducted a subscale live demonstration of certain critical aspects of the BSX candidate design. The HF radios and their magnetic antennas were one critical element in this testing, selected because they are the principal component-level difference from the Army system mentioned above. This demonstration validated the above-summarized assumptions about the performance of HF radio with the magnetic antennas. The BSX team also successfully performed a live performance-measurement field test using a pair of UHF radios.

As part of the design validation, the development team collected quantitative data on HF NVIS radio performance. Given the ranges and packet-completion rates provided therein for HF NVIS and the measurement results with the UHF radios (together with comparable radio performance data for UHF), estimates were made for BSX system-level performance by using system-modelling methodologies.
The results of this design validation process were quite consistent with expectations, fully supporting the BSX architecture and system design approaches, and indicating the BSX system should perform very well. For additional validation, the modelling and data were also evaluated in comparison with similar capabilities of the above-described U.S. Army system, whose architecture is similar.

C. Hosted Data Processing

This section considers the key data and processing elements to be hosted by the BSX platform. Specifically, the section examines the situational awareness data that BSX users will want and need, its bandwidth hosting requirements, and design approaches for engaging users with that data. As a communications platform, BSX will be capable of hosting other software applications; however, in consideration of innate Black Sky environment requirements and communications capacity limitations, it is important to ensure that this is limited to only the most vital software systems. The key data and software elements that BSX is designed to support are detailed here.

1. BSX Hosted System Data: Hosting Requirements for SAND™

This sub-section considers the question:

“What data will the users of the BSX system need to accomplish their mission of guiding and implementing sustainment and restoration operations?”
During a Black Sky outage in the continental United States, the Federal, state, local, tribal and territorial emergency management communities will be tasked with providing support to a large population, for an extended period of time, over a large geographic region. Such an event would cause unprecedented disruptions to essential services, not only within the power sector, but also for transportation, water, wastewater, healthcare, communications, and essentially all other infrastructure, resource, and service supply sectors. As discussed above, availability of the communications systems that these organizations use every day will be limited to a few hours or, at most, a few days following a Black Sky event.

To help the planning efforts for recovering from catastrophic outages, a systems analysis approach was used to identify the data requirements for Black Sky operations across multiple disciplines required to support infrastructure restoration and sustain populations in such scenarios. These data requirements are included as part of the SAND™ system, to be hosted by the BSX tactical network. SAND will provide a sensing and reporting framework to supply essential situational awareness data to decision makers and service providers when it is least available, yet most necessary.

As a result of this analysis, Black Sky operational mission requirements were developed, corresponding to three mission-critical functions.

**Black Sky Operational Mission Requirements: Mission Critical Functions**

- Execution of Strategic Mission Priorities
- Cross-Sector Planning and Coordination
- Resource Request and Acquisition

The corresponding information requirements were organized based on the use-case for this information, addressing each of the three mission-critical functions. Information types include:

- Event Characterization
- Consequence Analysis
- Decision Support

The development team then aligned data requirements (individual data elements) with each information requirement to define the most appropriate and comprehensive source of that information. Data requirements represent
the underlying granular datasets (e.g., infrastructure of concern in the impacted area, or population with durable medical equipment) needed to meet each information requirement. Most information requirements are fed by multiple data requirements, representing the collation of those data into response-relevant information that is operationally useful. Each data requirement was described by its relative information transfer load within a Black Sky-functional communications system, in terms of the number and type of fields required for tabular data and text, and the number and type of geospatial elements and metadata fields required for maps.

These specifications allow the total relative data load requirements for a communications system to be estimated, which then allows the total data requirement to be compared to the capacity provided by the proposed emergency communications system.

2. Information Management Framework

In Black Sky emergency response efforts supporting the “whole of community,” an information management framework is required to serve the operational coordination and management functions required of the emergency management community at all jurisdictional levels. The primary management requirement during a Black Sky event, or any other emergency, is to understand the situation, what tasks are required to mitigate losses, and the process by which the response and recovery efforts can most effectively mitigate those losses. The primary coordination task is to determine how organizations can best work together to coordinate the prioritized delivery of services to support the “on the ground” operational response and recovery apparatus of private and public organizations.

The proposed BSX data coordination approach explicitly respects the roles and responsibilities of each organization and asset owner to execute Black Sky emergency plans within their respective chains of command, while also addressing the need for national-level coordination.

This coordination involves multiple sectors and requires macro-level alignment of planning and preparatory efforts. Notably, this section posits that macro-level coordination may co-exist with micro-level coordination, defined as that which is managed from within an organization that may have greater tolerance for traditional communications-and-coordination approaches.
Therefore, the proposed approach to effectively manage and coordinate Black Sky response efforts includes the definition of clear operational mission requirements that shape and drive the functions of management and coordination, as well as data requirements that serve the missions of national, regional, and local efforts.

3. **Data Analysis: Based on the FEMA Response Federal Interagency Operational Plans (FIOPs)**

For this analysis, the Black Sky operational phases were drawn directly from the FEMA Response Federal Interagency Operational Plans (FIOPs). The FIOPs are built upon the concepts outlined in the National Response Framework and serve as operational documents specifying how various Federal agencies work and interact to support national preparedness. There are five FIOPs, each describing one of the preparedness mission areas: Prevention, Protection, Mitigation, Response, and Recovery.

The National Response Framework and the five FIOPs articulate a comprehensive vision of how the numerous agencies comprising the preparedness community can work together using common language and operational procedures, thereby aligning their mission-specific practices with those of the overall community. In support of this integration strategy, the three emergency management phases (e.g., steady-state, response, and recovery), and eight sub-phases used in this document have been pulled directly from the FEMA Response FIOP, as illustrated in figure G, below:

![Figure G | FIOP phases of emergency management.](image)

---


For each Black Sky operational sub-phase, a series of three information categories was provided to broadly scope and define the related operational information and data requirements. These three information categories are: event characterization; consequence analysis; and decision support.

Event characterization models and analyses convert raw observational data into situational awareness information describing the location, timing, and/or severity of an event. Event characterization performed prior to a hazardous event may predict, for example, the cities or regions likely to be affected and to what degree. Event characterization may occur before, during, or following an event to support long-term planning for a hypothetical event, rapid assessment of an ongoing event, or extent validation of an event which has already occurred, respectively.

The actions that must be completed are summarized by the various coordination and decision-making entities after a Black Sky event, in order to support infrastructure restoration and population sustainment. Each of these actions requires certain data, which were identified in the design process.

A detailed analysis was then conducted on those data:

- Users of the information
- Name of the information item
- Description of the information item
- Whether this information item is likely to be required, or only desired
- Form the information item will take
- Frequency of measurement or data acquisition required to support the mission
- Accuracy / quality requirements
- Source(s) for this information item
- Rationale for the need / desire for this information item

4. BSX Data Processing: Hosting Requirements for GINOM™

The data discussed above will be essential as a basis for decision makers and service providers to “manually” replicate and repair the systems and processes that normally provide critical services and resources. Nevertheless, in practice, these individuals will require significant “machine assistance” in order to successfully replicate even a portion of these highly complex, autonomous, and interconnected functions.
The GINOM™ software package, currently in development, is being designed to fill this need while operating within the data capacity limitations of the BSX communications platform. Utilizing the SAND situational awareness framework to acquire the required data, GINOM will need to consume and process this diagnostic data to provide user-friendly situational awareness information and decision support, mapping out complex infrastructure supply chain interdependencies and forecasting the consequences of particular resource allocation plans.

5. Effective and Suitable

The challenge of building a user-friendly system, however, is not an insignificant one. One might assume that the success of such a system would be based exclusively on the value of the information that it supplies to its users. However, while the quality of that information is important, it will not be the most critical factor in determining whether or not the system proves successful.

An insightful statement from the Federal Acquisition Regulation (FAR) illustrates this point. The FAR states that a system should not be fielded until it has been found to be both “effective” and “suitable.” By using this phrasing, the FAR acknowledges that a system could be effective without being suitable, or suitable without being effective. In this context, “effective” means that the system meets its established specification; this is an objective assessment that all mandatory requirements have been successfully implemented and verified.

---

through an appropriate test program. “Suitable,” on the other hand, means that the system is appropriate for its intended purpose and users.

Experience indicates that this concept of “suitability” is vital to the success of users depending on complex systems such as BSX, SAND, and GINOM. This is inherently somewhat of a subjective assessment: Do users like it? Can the system be operated in the actual highly-stressful environment for which it is intended, by the actual users (given their knowledge and skill)? Is the system consistent and reliable? Does it respond quickly to user commands? Can it do all of these things without putting an undue burden of computer science expertise onto those users? Can it do all of these things at the scale necessary (i.e., 200,000+ points of BSX presence and millions of components in the infrastructure network supply chain)? Can it do so while providing the necessary very high level of reliability?

If a system passes these tests, experience repeatedly indicates that such a system will be liked and accepted by the user community and utilized operationally. The information content (even if not ideal in its initial instantiation) can be adjusted over time based on feedback from those users. But if the system fails these tests, it does not matter how complete the information that could be displayed is; it will not be liked, trusted, or operated appropriately during actual emergency operations.

In this regard, while it remains essential to understand what data will effectively allow emergency management and service providers to perform their missions, assuring that the BSX-hosted, combined SAND and GINOM systems highlight and provide data and associated decision support that is suitable will be a greater technical challenge. To be sure, it will be crucial to achieve both. The insight offered by the aforementioned portion of the FAR, however, is that one must focus separately on both of these goals; accomplishing one does not automatically result in accomplishing the other.
6. Key goals and challenges for achieving a BSX-hosted system of systems that is both effective and suitable

This sub-section addresses the key goals and challenges in making the BSX and the hosted SAND and GINOM systems suitable, as well as effective for its intended users.

Consider the following summary of planning and response task categories to be performed by GINOM, supported by the BSX system:

a. Black Sky preparatory task categories
   - Black Sky Protocols: Pre-plan Black Sky day tasks and actions, i.e., outline of emergency restoration tasks for infrastructure personnel to sustain and restore critical services, and for emergency management to coordinate response operations.
   - Black Sky Training: Support training scenarios to allow emergency personnel to practice coordinated Black Sky plans in a risk-free environment.

b. Real-time, post-event task categories
   - Critical, Real-Time Events: Provide a continuously updated “ground truth” model identifying events that are “on the critical path” for mission effectiveness as conditions change and restoration proceeds, allowing for effective coordination.
   - Interdependency Mapping: Provide network analysis tools to track in-sector and inter-sector supply chain pathways to inform efficient prioritization of resources.
   - Prioritization / Decision Support: Forecast effects of potential resource prioritizations on the complex infrastructure supply chain to support alignment of recovery plans with dynamic “ground truth.”

Emergency managers and operations personnel in all major sectors will be the key users of an emergency communication and coordination “system of systems:” the BSX network, and the SAND and GINOM systems it hosts. The users of this system of systems will include two primary groups:

- Those whose tasks relate primarily to coordinating the recovery action, but who do not personally take actions to restore service; and
- Those whose tasks relate primarily to specific actions to restore service.
Operators within two defined role categories will require substantially different information and tools in order to be successful.

c. Information requirements and tools, as a function of user role

- **Users providing coordination functionality:** The Need for a Coordination Interface
  Those who are coordinating and communicating about recovery efforts will need status information, analysis, and planning tools. This may include: visualization of systems’ operational status; tools for tracking cross-sector supply chains; resource requirements for recovery operations; estimates about task completion times; resource provider information; forecasting services to predict overall effects of task prioritizations; etc.

- **Active users, “in the field:”** The Need for a Task Management Interface
  Those who are performing the actual recovery efforts will need information about the tasks themselves. This may include: prioritized task lists for recovery operations (e.g., black start); lists of emergency resource suppliers (people, parts and equipment, and information) for each task; a system for coordinating whether all necessary personnel and resources are in place to perform coordinated tasks; a means to record what has been completed for feedback through SAND back into the GINOM database; etc.

  Most detailed planning must occur long before a Black Sky event. Yet, real-time tasks must be dynamically added and removed depending on the state of critical supply chains. This constantly-updated operating picture will need to be synchronized across all GINOM clients in order to avoid potentially crippling disorder and inefficiencies.

These views – a coordination interface and task management interface – therefore become the core windows into the GINOM system. Each of these will provide user-tailored insight into the tasks at hand based on an underlying framework that is constantly tracking changes to the overall system state, maintaining a digital copy of the “ground truth,” and providing analysis and network forecasting services.
Much of the detailed planning for recovery tasks can only be performed long in advance of the emergency – both with regard to task definitions and the necessary trained personnel and equipment required to complete them. Yet, during the actual emergency, the priority of tasks will need to be adjusted as a function of the overall scenario. Tasks will be dynamically added and removed depending on the current supply chain state, creating new relationships within the network. This constantly-updated picture will need to be synchronized across all BSX and GINOM clients in order to avoid potentially crippling disorder and inefficiencies.

The synchronized operating picture will also be critical in informing coordination with relevant stakeholders, including political authorities (and through them, the general public), police and fire departments, and NGOs operating in the area. This operating picture will also inform decision-makers of the status of the parts, equipment, information, and personnel needed to undertake recovery actions. It will thereby allow for the facilitation of recovery efforts, both by those at higher echelons of government and those outside of the affected area.

In this regard, while the SAND and GINOM software will necessarily be decoupled from the BSX platform from a technical standpoint, their suitability will be tightly linked. While reliable communications are a core requirement of any recovery operation, effective recovery will depend on both meaningful data and a coordination and planning system to keep complex, distributed efforts in sync.

Conversely, these diagnostic data and coordination systems will be useless without a reliable communications platform synchronizing situational awareness and task prioritization among the emergency management and service provider user base. Together, the BSX, SAND, and GINOM platforms will thereby constitute a tiered, hardened restoration and sustainment framework for extreme events.
Fortunately, the U.S. has yet to face an event that triggered subcontinent-scale outages. The procedures and standards that currently facilitate power restoration have been shaped by decades of experience with outages at the city, state, and regional levels. However, as we continually upgrade our critical infrastructure systems to increase their scope and improve efficiency, we create a new class of vulnerabilities as expanding interdependencies and decreasing overall resilience lead to heightened potential for cascading failures.

Because we have not had to face an actual event at this scale, there is little “push-back” to widespread efforts towards increasing efficiency at the expense of resilience in our critical societal systems. As a result, any major attack or natural event that disrupts elements of the electrical grid on a multi-region scale will present challenges that greatly differ from those that existing restoration systems have been designed to combat.\(^{40}\)

For this reason, a coordinated recovery framework supporting emergency communications, diagnostic data acquisition, situational awareness, and decision support will be essential as society continues to move forward.

---

D. Networking Rule-Sets

Clear, prioritized networking rule-sets will be critical to ensure BSX fulfills its intended function. These rule-sets will be essential for managing communications and data transfer over what, in time, will become the BSX network. The rule-sets will necessarily need to be enforced autonomously to ensure seamless operation for all users. This section, therefore, reviews key aspects of the BSX network configuration, and hidden automation processes designed to balance ease of use and reliability in the BSX system.

In particular, in a Black Sky outage, the nation will be depending on the BSX system to host an interactive restoration and sustainment process of unprecedented complexity. In a subcontinent (or larger) scale blackout, BSX and the situational awareness and decision support systems it will host will need to support widely-dispersed decision makers in mediating recovery operations spanning tens of infrastructure sectors and a vast array of supply chains. The system will also need to ensure the delivery of resources critical to public health and safety to sustain the affected population, all in a highly disrupted environment.

When users log into the BSX network management system, the system will characterize them based on embedded data. This data includes: their location, BSX assets available, their roles in use of the network and in the overall recovery process, and the relevance of those roles to their location. In coordination with situational awareness and decision support guidance from the hosted SAND and GINOM systems, this allows the BSX to adjust available network resources, and support overall use of the system.

1. Network Management and Operation

The BSX network, as described above, will depend on radios as its primary communications link-bearers. Radio systems have great flexibility in
emergency operations, as system operators do not need to define all network nodes in advance. That very flexibility, however, introduces complexity in the establishment and maintenance of the network configuration.

To address this complexity, the system itself needs to automatically perform these establishment and network configuration tasks. This will shift the inherent complexity of network configuration from system users to the system developers. This is a non-trivial task, and therefore forms one of the key aspects of the design, aimed at making the BSX both suitable and effective.

This capability is implemented via specialized software which builds and maintains linkages between the various BSX sites.

a. Communication linkage types between BSX users

- One-to-one voice communications
- Voice conferencing
- Reporting and collection of a limited set of machine-to-machine data, e.g., SCADA signals
- Operator-initiated data messages, including status reports, task assignments, movement and re-supply planning and status, etc.
- Automatic data messages that synchronize databases at different sites

The network management and operations software will accomplish the following tasks:

- Find and build “paths” to other BSX nodes, adjusting over time as the system configuration changes
- Allocate (limited) network bandwidth to the various types of services and missions, including:
  - Voice
  - Data
  - Task management
  - Meetings / calendaring
  - Movement and re-supply planning
  - Background tasks (e.g., machine-to-machine coordination)

These tasks will be performed in conjunction with other capabilities described in previous sections, and while providing a security/authentication overlay suitable for the Black Sky mission.
b. Layered network architecture

Achieving a survivable, widely deployed communications system independent of any existing legacy infrastructure requires a layered network architecture. While each of these layers are relatively simple, they combine to provide a robust data transmission capability. These layers include single-hop reliability, frequency selection, communications path diversity, and multi-hop communications, each of which is described below.

i. Single Hop Reliability

The success rate of single-hop, direct site-to-site radio-based communications is seldom adequate for providing reliable network operations. It is common practice, therefore, to allocate a small additional portion of the available communications capacity to a mathematical coding scheme that can detect and automatically correct errors in the data stream. This technique is called error-correction coding. Within BSX, this error-correction coding will be combined with packet-level correction protocols: the information to be sent is separated into small sections (“packets”), and the failure of the packet to arrive correctly can be detected. If the error-correction coding cannot reconstruct the correct version of the packet, the system can automatically request that the single missing or incorrect packet be re-sent.

Through a combination of such mechanisms, the single-hop, direct site-to-site communications success rate can be improved to the desired level using only a small portion of the available communications capacity. These techniques are implemented in the packet router located at each BSX site.

ii. Radio selection

Each BSX site will house two independent radios, on different frequency bands, utilizing different radio modulations. This provides an important level of communications path diversity, and further improves system reliability.

The router at each site determines which radio to use for each transmission attempt (for both voice and data) based on its radio
“visibility” to adjoining sites. No manual action is required by the BSX operator to make this selection, which is implemented in the packet router located at each BSX site.

iii. Multi-hop communications

The packet router uses the same visibility information to implement multi-hop communications for both voice and data, allowing communications links to be established through the use of intermediate nodes.

iv. Frequency and modulation selection

Particular radio transmission frequencies and modulations will work better in some atmospheric conditions than others. The BSX network will select frequency and modulation based on time-of-day, atmospheric conditions, and other factors. An intelligent director controls and coordinates this process, providing direction to the packet routers at each BSX site. The local packet routers in turn command the radios to use the appropriate frequencies and other radio settings. No manual action is required by BSX operators to account for frequency and modulation preferences.

In addition to transmission considerations, radio frequency spectrum is a shared resource whose use is governed by Federal law and regulation. The BSX network’s frequency utilization policy will be coordinated with regional and national civil officials. In fact, the rules governing frequency utilization are different during major emergencies than during nominal times. The network must account for these differences, limiting its frequency use during nominal situations (e.g., during routine training and testing activities) to the frequencies and transmission power levels allowed during normal situations.

The system, however, will take advantage of the larger range of frequency and transmission power levels permitted during emergency situations. The appropriate regional and/or Federal officials may allocate or de-allocate the use of certain radio frequencies as a situation evolves in order to de-conflict the use of particular radio frequencies; BSX must be able to accept such frequency-utilization guidance during emergency operations. These
capabilities are also implemented within the intelligent director. No manual action is required by BSX operators to comply with such changes in radio frequency policy.

2. Operating Within Available Network Capacity

All electronic communications systems have capacity limits. Even when operating at full capacity, there is a maximum amount of data that can be moved per unit of time. Some communications systems have different capacity limits for short and long-term periods, akin to the difference in speed achieved by someone running a mile, as compared to that person running a 100-yard dash.

Given knowledge of the data that will be moved around the system, and a model of where and how frequently each item must be moved, one can create a model of information flow. From this model, predictions of the necessary communications capacity can be derived.

It is also the case, however, that not all techniques for organizing, formatting, and moving the data impose the same demands upon the electronic communications system. There are, in fact, a variety of techniques that move the data around in a fashion that uses less data capacity than others. This section identifies a set of such techniques that are appropriate for the BSX system. These design techniques will allow BSX users to accomplish their missions within the limitations of the communications devices and networks described in previous sections.

In addition to improving the network’s overall capacity, the BSX network will also utilize optimization techniques to reduce the overall requirements for such capacity. Techniques available include bit-oriented messaging, multicast transmission, and dynamic allocation of bandwidth to users, missions, and data categories.
E. BSX Network Power Management Options

With grid power unavailable over large areas, BSX nodes will need to include provisions to ensure adequate emergency power will be available for 30 to 60-days of operation. Mobile, truck-based nodes will typically utilize power generated by the vehicle’s alternator to operate the BSX communications package. For conventional gasoline-fueled trucks, the vehicle’s (enhanced) alternator would provide power, depending on the truck’s fuel tank for energy storage. For sites using mobile nodes, logistics planning for vehicle fuel would need to take such use into account.

For fixed site deployment, however, the BSX system will address this need through a combination of different approaches. The approach for a given site will be selected based on the overall needs for the emergency communications network, and on the specific needs of each node within its hosting facility. These network power management approaches include node/facility power budgeting, and the provision of a range of supplemental power module configurations, subject to user requirements.

1. BSX Network Power Management Planning: Node / Facility Power Budgeting

In reviewing the power budget for BSX nodes, radios entail, by far, the highest power utilization. Computers and other devices in a given node will require far less power. This represents an important opportunity for overall network power management, which will be incorporated as a basic feature of the full-scale network management system.

In particular, using projected facility power availability at each node as a key parameter, the BSX network system will coordinate adjustments to the “duty cycle” of radio use for each node. These adjustments will be further configurable according to GINOM or user-forecasted requirements for increased communication windows.
As a simple example, some facilities are not staffed for portions of each day; radios at these nodes will not be powered on when the facility is vacant. In the more general case of continuous staffing, the duty cycle of a node's radio availability will be a key data point provided to the overall BSX network management system. Users attempting to communicate with such facilities will be alerted as to their next “window” of availability. Initially, this may be implemented by using a “baseline duty cycle” for all nodes with limited power storage capabilities, with all such nodes sharing a common “on” window for coordinated messaging. Over time, BSX network management software, with guidance based on configured operational need, can provide far more sophisticated allocation.

This approach can substantially cut the overall power needs for nodes “challenged” by available stored power. However, such limitations may not be required for many nodes due to the continued availability of adequate emergency facility power.

a. **Baselining Emergency Power Requirements at Critical Facilities**

The starting point for defining power requirements for the overall BSX network as well as individual nodes is to consider the availability of emergency power at the primary facilities that will utilize the system.

In each infrastructure, government, and NGO sector, and for major corporations in critical supply chains, the most urgent need for BSX nodes will be at critical operations, dispatch, control, and coordination facilities. For major service providers like hospitals, government institutions, and security offices, co-location in the primary facilities of such service providers will be essential.

In each of these cases, basic operation of the facility itself – that is, its ability to perform its fundamental mission, separate from its need for...
emergency communications – will require secure, continued availability of emergency facility power for the 30 to 60-day period identified above.

This represents a significant change from current standard practice. Yet, this will be essential to allow such facilities to perform their critical Black Sky restoration and sustainment missions. Though not representative of today’s reality, evolution to meet this need must be accommodated by new public and private sector Black Sky policy, doctrinal changes, and investments if such critical facilities are to be capable of supporting the restoration and sustainment roles that they, uniquely, will serve.

b. Matching BSX Power Needs to Anticipated Emergency Facility Power

While the overall power needs for BSX nodes can be “adjusted” by the network’s management software through changes in factors like radio duty cycle, nodes at critical facilities may have far less constraining requirements. Deployment of nodes in such facilities will need to include an assessment of the facility power budget. If the facility’s emergency power source(s) can adequately meet BSX requirements in addition to other essential functions, the BSX node’s radios can operate at a 100% duty cycle without the need for supplemental power modules (other than for backup purposes).

2. BSX Network Power Management Planning: Supplemental Power Module Configurations

For smaller fixed site facilities that require a BSX node, facility power may only be intermittently available, or too low to provide a significant portion of the BSX node’s needs. In these cases, the BSX node will be accompanied by a supplemental power module, with the user deciding – based on the particular facility’s needs – the type and size of module required.

A renewable power source such as solar cells may also be used to add additional capability, depending on user requirements. This option, reviewed in detail below, is applicable for both supplemental power module configurations.

a. Conventional Emergency Power Devices

As one example, users may choose to utilize conventional emergency power solutions, such as emergency generators. Some emergency generator configurations may have limited operational lifetimes, and this must be accounted for in the selection process.
In addition, most commonly-available generators utilize diesel fuel. There are various considerations which may make storage of 30 day+ supplies for these generators difficult or impractical – especially due to the limited storage life of diesel fuel and limits to on-site storage imposed by building and operating permits at many facilities. However, with most large-scale critical facilities likely to depend on emergency diesel generators for years to come, the new Black Sky coordination frameworks discussed in Chapter I will need to develop planning for nationwide distribution of such fuel as a primary priority, and this may make diesel generators for some BSX nodes more practical.

Emergency generators using compressed natural gas storage are also available, which may offer another alternative. This fuel does not have the same short storage lifetime limitations associated with diesel.

**b. Long Duration Battery Power**

Given reliability and fuel limitations for conventional supplemental power configurations, the BSX design team developed an additional option: a long duration battery storage configuration.

For the busiest BSX sites, estimated total power requirements for a 100% duty cycle with heavy use in transmission mode would be a maximum of 28 KWh per day, as shown in Figure H. Actual deployment decisions may take into account anticipated duty cycles of radio use and/or expected use in power-intensive transmission vs. simple monitoring modes. As discussed above, duty cycle timing may also be pre-determined by decision makers to arrange for pre-planned operating periods, distributed throughout the day.

For a 30-day capability with no secondary power source (such as solar), a heavy use site working at a 100% duty cycle will require a power source
sized at just over 800KWh. Most of the BSX sites, however, will likely require much less power capacity due to a significantly lower duty cycle anticipated for use of their radios – the primary power drain for a node – or for those operating mostly in “monitoring” mode.

3. Battery Technology Options

There are multiple current options available for users who require a substantial, battery-based power module. Additional options may become available over time. Battery technology, however, has generally advanced far slower than electronics technology; the system should therefore not rely on dramatic improvements in batteries. Nevertheless, current battery options include:

a. Li-ion batteries

The 129 MWh Powerpack battery, provided by Tesla, integrated into the power grid in South Australia. While far larger than required for the purposes of BSX, this installation illustrates the scalability of Li-ion battery technology. | Image: Tesla

While constrained by limits on the number of charge / discharge cycles they can support, Li-ion batteries (LIB) are increasingly used in the power industry, and widely used commercially. For example, the 129 MWh Powerpack project in South Australia, currently the largest battery in the world, is designed as a “virtual powerplant” with capacity orders of magnitude larger than required for BSX.41

At a more appropriate size, Tesla’s LIB “Powerwall home battery”, for example, provides 13.5 KWh. Four such units, advertised by Tesla at a total retail cost of approximately $25K, would fit within a half cubic meter volume, providing over 50 KWh of capacity.

<table>
<thead>
<tr>
<th></th>
<th>One Day</th>
<th>30 Days</th>
<th>60 Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Power Requirement (KWh)</td>
<td>24.00</td>
<td>720.00</td>
<td>1,440.00</td>
</tr>
<tr>
<td>Computer Power Requirement (KWh)</td>
<td>2.0</td>
<td>60.0</td>
<td>120.0</td>
</tr>
<tr>
<td>Total Losses</td>
<td>1.68</td>
<td>50.40</td>
<td>100.80</td>
</tr>
<tr>
<td>Inverter Losses (5%)</td>
<td>1.20</td>
<td>36.00</td>
<td>72.00</td>
</tr>
<tr>
<td>Transmission Losses (2%)</td>
<td>0.48</td>
<td>14.40</td>
<td>28.80</td>
</tr>
<tr>
<td>Implied total BSX Power Capability (KWh)</td>
<td>27.68</td>
<td>830.40</td>
<td>1,660.80</td>
</tr>
</tbody>
</table>

Figure H | Power Capability Estimate for BSX Nodes

b. Flow batteries

Flow batteries were another alternative evaluated by the BSX design team. Vanadium Redox flow batteries, commercially available at costs similar to LIB technology for comparable capacity, have certain advantages. While requiring a far larger volume / deployment footprint, such flow batteries have both much longer storage life and a lower charging degradation cycle

than Lithium ion batteries,\textsuperscript{43} which will be significant considerations for some BSX users. Vanadium redox batteries are commercially offered by companies such as UniEnergy Technologies\textsuperscript{44} and Schmid.\textsuperscript{45}

In particular, the primary advantages of vanadium redox flow batteries include:

\begin{itemize}
  \item Simple energy capacity scaling, through use of larger electrolyte storage tanks
  \item Batteries can be stored fully charged for long periods without degradation
  \item If electrolytes are accidentally mixed, the battery suffers no permanent damage
  \item A single state of charge between the two electrolytes avoids the capacity degradation due to a single cell in non-flow batteries
  \item The electrolyte is aqueous and inherently safe and non-flammable
  \item The generation-3 formulation, using a mixed acid solution developed by the Pacific Northwest National Laboratory, operates at a high temperature, allowing for passive cooling\textsuperscript{46}
\end{itemize}

\begin{footnotes}
\end{footnotes}
- Maintenance requirements are also low. As an example, backup pumps may be stored at the site in the event that the system's pumps fail and need to be replaced.

In all, the BSX design team evaluated more than 20 battery chemistries. Other battery technologies may become available, over time. As an example, Zinc Air batteries currently in development for BSX nodes. These metal-air batteries, powered by oxidizing zinc with oxygen taken from ambient air, promise relatively high energy densities and are said to be relatively inexpensive to produce.

For typical, fixed site nodes, flow battery technology was selected as the optimal for a long duration battery-based supplemental power module.

For typical, fixed site nodes, flow battery technology was selected as the optimal for a long duration battery-based supplemental power module.


c. Supplemental Solar Cell Power Supply

For those nodes and node clusters with basing anticipated in appropriate climatic zones, BSX power modules will include solar panels to complement battery energy storage and reduce the required size of the battery package. As an example, using the average U.S. solar power density of 4.5 kWh/m2/
day, placing solar panels on top of a standard 20-foot shipping container (14 m² surface area) would yield about 63 kWh/day. The actual electricity generated by these solar panels, however, varies materially depending on geographic location (see Figure H for typical solar-resource at various locations across the U.S.). A flow battery solution in this same shipping container form-factor could easily provide 45 kWh/day. A LIB battery of comparable capacity could fit in a far smaller volume, making rooftop deployment for solar panels a likely approach for such configurations.

Therefore, the 63 kWh/day solar configuration, together with suitable battery storage, would provide more than adequate continuous emergency power indefinitely for the 100% duty cycle case of 28 kWh per day at a given site. Any battery configuration of this capacity would provide a 38-hour reserve for periods with minimal or no sunlight. Correspondingly, for lower duty cycles (e.g., the 10 minute / hour example), this configuration would allow for substantial margin to address reduced solar availability periods or other contingencies.

Figure H | U.S. Photovoltaic solar resource maps.
Wind power systems may also be utilized in appropriate locations and could supplement BSX power modules in regions where site surveys find that surging winds of >15 mph are relatively common. However, the dependence of wind power systems on moving parts results in far shorter storage lifetimes, lower availabilities, and higher maintenance requirements than approaches without such a dependence.

Site-specific designs (see Figure H, which uses data from the National Renewable Energy Laboratory and U.S. Department of Energy) would lead to optimal sizing of BSX power elements at each specific facility, and final selection from the mix of approaches reviewed above.

As reviewed in Chapter I, national continuity through Black Sky outages will require thorough, well-coordinated planning spanning most infrastructure, resource, and service sectors, and their government and mass-care NGO partners. However, that same well-integrated multi-sector coordination will need to continue in real time following a Black Sky event to guide infrastructure restoration and population sustainment.

With all normal telecommunications, internet, and related services offline, this will only be possible if nations deploy a Black Sky-compatible emergency communications system to interconnect nearly all sectors, including key segments of their supply chains. Yet even with such a system, “manual” guidance on subcontinental scales – without the autonomous processes that normally provide all of society’s goods and services – will be impossible without multi-sector situational awareness and decision support.

Developing, implementing, and deploying such a system – designed to survive a long duration outage and continue to operate without depending on
a functional power grid or normal, national telecommunications assets – is a fundamental test of the credibility of a nation’s national continuity planning and national security, broadly defined.
Appendix
Appendix A
Emergency Support Functions and ESF Coordinators


ESF #1—Transportation
- **ESF Coordinator**: Department of Transportation
- **Key Response Core Capability**: Critical Transportation

Coordinates the support of management of transportation systems and infrastructure, the regulation of transportation, management of the Nation’s airspace, and ensuring the safety and security of the national transportation system. Functions include but are not limited to:

- Transportation modes management and control
- Transportation safety
- Stabilization and reestablishment of transportation infrastructure
- Movement restrictions
- Damage and impact assessment.

ESF #2—Communications
- **ESF Coordinator**: DHS/Cybersecurity and Communications
- **Key Response Core Capability**: Operational Communications, Infrastructure Systems

Coordinates government and industry efforts for the reestablishment and provision of critical communications infrastructure, facilitates the stabilization of systems and applications from malicious cyber activity, and coordinates communications support to response efforts. Functions include but are not limited to:

- Coordination with telecommunications and information technology industries
Coordination of the reestablishment and provision of critical communications infrastructure

Protection, reestablishment, and sustainment of national cyber and information technology resources

Oversight of communications within the Federal response structures

Facilitation of the stabilization of systems and applications from cyber events.

**ESF #3—Public Works and Engineering**

- **ESF Coordinator:** DOD/U.S. Army Corps of Engineers
- **Key Response Core Capabilities:** Infrastructure Systems, Critical Transportation, Logistics and Supply Chain Management, Environmental Response/Health and Safety, Fatality Management, Mass Care Services, Mass Search and Rescue Operations

Coordinates the capabilities and resources to facilitate the delivery of services, technical assistance, engineering expertise, construction management, and other support to prepare for, respond to, and/or recover from a disaster or an incident. Functions include but are not limited to:

- Infrastructure protection and emergency repair
- Critical infrastructure reestablishment
- Engineering services and construction management
- Emergency contracting support for lifesaving and life-sustaining services

**ESF #4—Firefighting**

- **ESF Coordinator:** USDA/U.S. Forest Service and DHS/FEMA/U.S. Fire Administration
- **Key Response Core Capabilities:** Operational Communications Logistics and Supply Chain Management, Infrastructure Systems On-Scene Security, Protection, and Law Enforcement Public Health, Healthcare, and Emergency Medical Services, Fire Management and Suppression, Situational Assessment

Coordinates the support for the detection and suppression of fires. Functions include but are not limited to:

- Support to wildland, rural, and urban firefighting operations.
**ESF #5—Information and Planning**
- **ESF Coordinator:** DHS/FEMA
- **Key Response Core Capabilities:** Situational Assessment, Planning, Public Information and Warning

Supports and facilitates multiagency planning and coordination for operations involving incidents requiring Federal coordination. Functions include but are not limited to:

- Incident action planning
- Information collection, analysis, and dissemination.

**ESF #6—Mass Care, Emergency Assistance, Temporary Housing, and Human Services**
- **ESF Coordinator:** DHS/FEMA
- **Key Response Core Capabilities:** Mass Care Services, Logistics and Supply Chain Management, Public Health, Healthcare, and Emergency Medical Services, Critical Transportation, Fatality Management Services

Coordinates the delivery of mass care and emergency assistance. Functions include but are not limited to:

- Mass care
- Emergency assistance
- Temporary housing
- Human services.

**ESF #7—Logistics**
- **ESF Coordinator:** General Services Administration and DHS/FEMA
- **Key Response Core Capabilities:** Logistics and Supply Chain Management, Mass Care Services, Critical Transportation, Infrastructure Systems, Operational Communications

Coordinates comprehensive incident resource planning, management, and sustainment capability to meet the needs of disaster survivors and responders. Functions include but are not limited to:
- Comprehensive, national incident logistics planning, management, and sustainment capability
- Resource support (e.g., facility space, office equipment and supplies, contracting services).

**ESF #8—Public Health and Medical Services**

- **ESF Coordinator:** Department of Health and Human Services
- **Key Response Core Capabilities:** Public Health, Healthcare, and Emergency Medical Services, Fatality Management Services, Mass Care Services, Critical Transportation, Public Information and Warning, Environmental Response/Health and Safety, Logistics and Supply Chain Management

Coordinates the mechanisms for assistance in response to an actual or potential public health and medical disaster or incident. Functions include but are not limited to:

- Public health
- Medical surge support including patient movement
- Behavioral health services
- Mass fatality management.

**ESF #9—Search and Rescue**

- **ESF Coordinator:** DHS/FEMA
- **Key Response Core Capability:** Mass Search and Rescue Operations

Coordinates the rapid deployment of search and rescue resources to provide specialized lifesaving assistance. Functions include but are not limited to:

- Structural collapse (urban) search and rescue
- Maritime/coastal/waterborne search and rescue
- Land search and rescue.

**ESF #10—Oil and Hazardous Materials Response**

- **ESF Coordinator:** Environmental Protection Agency
- **Key Response Core Capabilities:** Environmental Response/Health
Appendix

and Safety, Critical Transportation, Infrastructure Systems, Public Information and Warning

Coordinates support in response to an actual or potential discharge and/or release of oil or hazardous materials. Functions include but are not limited to:

- Environmental assessment of the nature and extent of oil and hazardous materials contamination
- Environmental decontamination and cleanup, including buildings/structures and management of contaminated waste.

ESF #11—Agriculture and Natural Resources

- ESF Coordinator: Department of Agriculture
- Key Response Core Capabilities: Mass Care Services, Critical Transportation, Logistics and Supply Chain Management

Coordinates a variety of functions designed to protect the Nation's food supply, respond to plant and animal pest and disease outbreaks, and protect natural and cultural resources. Functions include but are not limited to:

- Nutrition assistance
- Animal and agricultural health issue response
- Technical expertise, coordination, and support of animal and agricultural emergency management
- Meat, poultry, and processed egg products safety and defense
- Natural and cultural resources and historic properties protection.

ESF #12—Energy

- ESF Coordinator: Department of Energy
- Key Response Core Capabilities: Infrastructure Systems, Logistics and Supply Chain Management, Situational Assessment

Facilitates the reestablishment of damaged energy systems and components and provides technical expertise during an incident involving radiological/nuclear materials. Functions include but are not limited to:

- Energy infrastructure assessment, repair, and reestablishment
- Energy industry utilities coordination
- Energy forecast.
**ESF #13—Public Safety and Security**

- **ESF Coordinator:** Department of Justice/Bureau of Alcohol, Tobacco, Firearms, and Explosives
- **Key Response Core Capability:** On-Scene Security, Protection, and Law Enforcement

Coordinates the integration of public safety and security capabilities and resources to support the full range of incident management activities. Functions include but are not limited to:

- Facility and resource security
- Security planning and technical resource assistance
- Public safety and security support
- Support to access, traffic, and crowd control.

**ESF #14—Superseded by National Disaster Recovery Framework**

**ESF #15—External Affairs**

- **ESF Coordinator:** DHS
- **Key Response Core Capability:** Public Information and Warning

Coordinates the release of accurate, coordinated, timely, and accessible public information to affected audiences, including the government, media, NGOs, and the private sector. Works closely with state and local officials to ensure outreach to the whole community. Functions include, but are not limited to:

- Public affairs and the Joint Information Center
- Intergovernmental (local, state, tribal, and territorial) affairs
- Congressional affairs
- Private sector outreach
- All Hazards Emergency Response Operations Tribal.
## Appendix B

### List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR</td>
<td>After-Action Report</td>
</tr>
<tr>
<td>BSPL</td>
<td>Black Sky Prioritization List</td>
</tr>
<tr>
<td>BSX</td>
<td>Black Sky Emergency Communications and Coordination</td>
</tr>
<tr>
<td>CSCC</td>
<td>Cross-Sector Coordinating Council</td>
</tr>
<tr>
<td>CIKR</td>
<td>Critical Infrastructure and Key Resources</td>
</tr>
<tr>
<td>CSIP</td>
<td>Cybersecurity Strategy and Implementation Plan</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOE</td>
<td>Department of Energy</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DMORT</td>
<td>Disaster Mortuary Operational Response Team</td>
</tr>
<tr>
<td>E-ISAC</td>
<td>Electricity Information Sharing and Analysis Center</td>
</tr>
<tr>
<td>EAGLE-I</td>
<td>Environment for Analysis of Geo-Located Energy Information</td>
</tr>
<tr>
<td>EEI</td>
<td>Edison Electric Institute</td>
</tr>
<tr>
<td>EMP</td>
<td>Electromagnetic Pulse</td>
</tr>
<tr>
<td>EO</td>
<td>Executive Order</td>
</tr>
<tr>
<td>EOC</td>
<td>Emergency Operations Center</td>
</tr>
<tr>
<td>EMAC</td>
<td>Emergency Management Assistance Compact</td>
</tr>
<tr>
<td>EPRI</td>
<td>Electric Power Research Institute</td>
</tr>
<tr>
<td>ESCC</td>
<td>Electricity Subsector Coordinating Council</td>
</tr>
<tr>
<td>ESF</td>
<td>Emergency Support Function</td>
</tr>
<tr>
<td>ESFLG</td>
<td>Emergency Support Function Leaders Group</td>
</tr>
<tr>
<td>FAST</td>
<td>Fixing America’s Surface Transportation</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency</td>
</tr>
<tr>
<td>FIOP</td>
<td>Federal Integrated Operational Plan</td>
</tr>
<tr>
<td>GINOM</td>
<td>Global Infrastructure Network Optimization Model</td>
</tr>
<tr>
<td>GMD</td>
<td>Geomagnetic Disturbance</td>
</tr>
</tbody>
</table>
HEMP  High Altitude Electromagnetic Pulse
HSPD  Homeland Security Policy Directive
HVA  High Value Assets
IAC  Integrated Analysis Cell
ICT  Internet and Communications Technology
IOC  Infrastructure of Concern
IoT  Internet of Things
ISAC  Information Sharing and Analysis Center
JFO  Joint Field Office
LPT  Large Power Transformer
MEF  Mission Essential Function
NBEOC  National Business Emergency Operations Center
NCIPP  National Critical Infrastructure Prioritization Program
NCIRP  National Cyber Incident Response Plan
NERC  North American Electric Reliability Corporation
NGO  Non-Governmental Organization
NICC  National Infrastructure Coordinating Center
NIMS  National Incident Management System
NIPP  National Infrastructure Protection Plan
NISAC  National Infrastructure Simulation and Analysis Center
NLE  National Level Exercise
NOC  National Operations Center
NRCC  National Response Coordination Center
NRF  National Response Framework
NSTAC  National Security Telecommunications Advisory Committee
OCIA  Office of Cyber and Infrastructure Analysis
OMB  Office of Management and Budget
ONG  Oil & Natural Gas
PCII  Protected Critical Infrastructure Information Program
PPD  Presidential Policy Directive
PSA  Protective Security Advisor
RRAP  Regional Resiliency Assessment Program
SCC  Sector Coordinating Council
SICC  Strategic Infrastructure Coordinating Council
SIEC  Strategic Infrastructure Executive Council
SSA  Sector-Specific Agency
THIRA  Threat and Hazard Identification and Risk Assessment
TSP  Telecommunications Service Priority
TTWG  Transformer Transportation Working Group
UAV  Unmanned Aerial Vehicles
UCG  Unified Coordination Group
USACE  U.S. Army Corps of Engineers
USDA  U.S. Department of Agriculture