Information Sharing

Guide for Private-Public Partnerships

September 2023

FEMA

Cover Image

The cover image shows a group of people representing organizations within a private-public partnership (P3) who are sharing information for the mutual benefit to enhance the life safety, economic security, and resilience of jurisdictions. The members of a P3 often share information through the human and technical systems of a partnership network, a community resilience hub, or a business emergency operations center (BEOC).

Acknowledgement:

The Information Sharing Guide for Private-Public Partnerships was developed adapting direct input from information sharing practitioners including the North Carolina Business Emergency Operations Center (BEOC), the Illinois BEOC, and the Nebraska Preparedness Partnership. Input from a variety of additional information sharing practitioners helped make the recommendations in this guide applicable for jurisdictions large and small.

This document contains references to non-federal resources. Linking to such sources does not constitute an endorsement by FEMA, the Department of Homeland Security, or any of its employees of the information or products presented.

Table of Contents

Introduction

Information is an asset that can improve situational awareness, operational readiness, and decision-making for building resilience. Information also assists in better managing disaster risk reduction, response, and recovery efforts. Jurisdictions need the private sector, public sector,[1] and non-governmental organizations (NGOs) to collaborate to strengthen information sharing capability and capacity before, during, and after a disaster or emergency. Building resilience is the foundation of private-public partnerships (P3) in emergency management.

1. Purpose

This guide provides recommendations and resources for any P3 to develop, conduct and improve the capability to share information for resilience,[2] response[3] and recovery. This guide is a continuation of concepts from the Building Private-Public Partnerships guide which introduces the importance of robust information sharing capabilities to improve whole community resilience.

- This guide helps a P3 to:
- Improve the ability to exchange intelligence, information, data, and knowledge;
- Improve the capability to manage and share information needed for:
    - Joint resilience, response and recovery planning, and strategy development;
    - Coordination of response and recovery operations; and
- Support joint messaging.

2. Target Audience

This guide is for any P3, whether private or public sector led, that shares information to improve resilience, response, or recovery operations. The members of a P3 often share information through the human and technical systems of a partnership network, a community resilience hub, or a business emergency operations center (BEOC).

[1] Public sector can also include National Guard.

[2] For this guide resilience includes mitigation, protection and preparedness.

[3] For this guide response also includes homeland security and law enforcement.

Examples of relevant stakeholder groups where private-public information exchange occurs include:

Information Sharing Partners

- **Private Sector Integration Program:** The Maryland Department of Emergency Management (MDEM) is a government led P3 model. MDEM incorporates private sector partners into the emergency management framework including during emergency operations center (EOC) activations, event information is shared via Maryland Virtual Business Operations Center and the Business Operations Center.[4]
- **Business Emergency Operations Center:** The Ohio Department of Public Safety established its BEOC to increase information sharing with the private sector. The goals are to improve visibility for the community lifelines and provide the information the state needs to provide a focused response. The BEOC also supports the private sector with information appropriate for business operations and continuity decisions.[5]
- **Community Resilience Hubs:** Resilience Hubs are facilities designed to distribute resources, coordinate information sharing and provide opportunities to increase interconnectedness and resilience within communities pre-disaster, during response, and during recovery.[6] Community-serving NGOs often serve as hubs and typically consist of a network of professionals.

3. Background

In the 1990s, many business leaders acted on the need to manage risks and information for crisis management and stay in business. Powered by good information, enterprise risk management emerged as a mission-critical concept, vital to crisis management.[7]

The Critical Infrastructure Information Act of 2002[8] focused federal support for the public and private sectors on gathering, communicating, or disseminating critical infrastructure information. A series of information-sharing programs and initiatives were formed in the years following. The Critical Infrastructure Partnership Advisory Council formed to facilitate the "sharing of information about

[4] For more information, see https://mdem.maryland.gov/Pages/psip.aspx.

[5] For more information, see https://homelandsecurity.ohio.gov/op3_files/2019/beoc.pdf.

[6] For more information on Resilience Hubs, see http://resilience-hub.org.

[7] For more information, see https://www.actuaries.org.uk/system/files/documents/pdf/03062015-birmingham-actuarial-society-enterprise-risk-management-event-enterprise-risk-management-it.pdf.

[8] For more information, see https://www.dhs.gov/sites/default/files/publications/CII-Act_508_0.pdf.

threats, vulnerabilities, protective and resilience measures, best practices and lessons learned" between private and public sector partners.[9] In 2012, FEMA established the National Business Emergency Operations Center[10] to support information sharing between private sector and the federal government.

The need for information sharing among the private sector, public sector and volunteer organizations was a lesson acted on by the American Logistics Aid Network after Hurricanes Katrina and Rita.[11] States such as Louisiana[12] and Illinois[13] built partnerships with businesses to share information, which led to creation of a state BEOC. In 2018 the All-Hazards Consortium[14] formed a secure information-sharing environment to facilitate information exchange between private and public sector organizations.

The 2019 National Response Framework added Emergency Support Function (ESF) 14–Cross-Sector Business and Infrastructure to facilitate operational information sharing between public and private sector organizations. From 2020–2022, states such as North Carolina, Illinois and Pennsylvania developed model plans and annexes to address private sector integration into emergency operations through information sharing.

[9] For more information, see https://www.cisa.gov/critical-infrastructure-partnership-advisory-council.

[10] For more information, see https://www.fema.gov/business-industry/national-business-emergency-operations-center.

[11] For more information, see https://www.alanaid.org/.

[12] For more information, see https://labeoc.org/more-about-us/about-us/.

[13] For more information, see https://iemaohs.illinois.gov/.

[14] For more information, see https://www.ahcusa.org/.

Case for Information Sharing

Private organizations, public organizations and NGOs often make decisions that require input from external sources based on information and analysis. During "blue-sky" and "gray-sky" events, a standard operational process is needed to build and sustain P3 information sharing and analysis.

1. Core Principles

Information sharing is the timely, accurate and actionable exchange of information between private organizations, public organizations and NGOs in multiple jurisdictions and disciplines. The following information sharing, and safeguarding core principles are described in this guide:

- **Information is an asset:** Information is an asset because it has real decision-making value and financial value that increases with the number of people who can either make it, use it or benefit from it;[15]
- **Decision-making requires timely, accurate, and trusted information:** Operational readiness and decision-making are the purposes of sharing information. Organizations that operate without all the information required to make decisions routinely make mistakes and fail to make optimal decisions to respond to a crisis or recover from a disaster; and
- **Collaboration ensures operational readiness:** Private organizations, public organizations and NGOs should plan to share and safeguard information and be part of collaborative information sharing activities to develop a common understanding of information to reduce risk, ensure readiness, and improve response and recovery.

2. Goals

The goals of P3 information sharing and safeguarding are:

- **Goal 1: Build trust and cooperation.** A P3 functions in the context of relationships. Sharing information is an expression of trust, a key ingredient required to form a relationship and facilitate ongoing cooperation necessary to exhibit openness and willingness to share information. Consistent application of information usage and safeguarding policies,[16] operations and technologies are integral to maintaining trust between and among partners;

[15] Adapted from https://www.techtarget.com/whatis/definition/information-assets.

[16] For more information, see https://www.cisa.gov/pcii-program; https://www.cisa.gov/circia.

- **Goal 2: Prioritize shared situational awareness and information analysis.** Situational awareness is the ability to identify, process and comprehend critical information about an incident. Shared situational awareness ensures that P3s understand the risks and vulnerabilities of the social and economic environment in which they operate, and ensures partners are using the same sources of information to better define and interpret the incident.
- **Goal 3: Enable sector-specific and cross-sector operational readiness.** The ability to establish accessible and consistent methods for information exchange support P3 partners to define how and when information shared can be incorporated into decision-making. Cross-sector information sharing should be conducted in near-real time to improve operational readiness. The nature and delivery of information should meet the functional and institutional needs of the partner organizations predictably and reliably. The readiness of people, processes and technologies is critical to the success of data-driven operations;
- **Goal 4: Facilitate joint decision-making.** Decision-making occurs within and among organizations. Information sharing is a vital resource that enables decision-making in business continuity planning, resilience operations, response and recovery missions, and critical infrastructure security.[17] Facilitation of rapid cross-sector and cross-disciplinary analysis and problem solving occurs when risk information, business status information, operational requests, and other industry insights are made available through shared services and interoperability;[18] and
- **Goal 5: Foster dynamic cross-sector collaboration to support mutual needs.** A P3 can harness the power of cross-sector collaboration by actively facilitating the exchange of information and valuable resources. This will cultivate an environment that not only meets mutual needs but also supports achievement of shared goals, enabling the government and private organizations to thrive.

3. Defining an Information Sharing Capability

For this guide, information sharing is the timely, accurate and actionable exchange of information between private organizations, public organizations, and NGOs in multiple jurisdictions and disciplines. Developing an information sharing capability is a multi-dimensional challenge because of various factors that impact the effectiveness and efficiency of sharing information across different entities. The following core elements will help P3s design and implement an information sharing capability.[19]

[17] Adapted from https://www.cisa.gov/information-sharing-vital-resource.

[18] For more information, see https://www.fema.gov/emergency-managers/national-preparedness/frameworks.

[19] For more information, see https://www.dhs.gov/sites/default/files/publications/IAS_IMIS-CMM-Framework_161220-508.pdf.

- Governance;
- Plans and standard operating procedures (SOPs);
- Technology;
- Training and exercises; and
- Usage.

An information sharing capability consists of the ability to perform certain functions and tasks described in **Appendix A:** Functional Information Sharing Model. **Appendix B:** Information Sharing Assessment Tool lays out a detailed self-assessment tool.

Building Information Sharing Capability

The best strategy is to build on what already exists and works to support information sharing for stakeholders. Information sharing supports decision-making at all levels, improving internal operations and effective execution of resilience activities. Developing a robust information sharing capability and capacity enables cross-sector collaboration and provides resources for critical infrastructure resilience.

1. Design

When designing the capability to share information it is crucial to consider the governance structure that supports and manages the process. Governance refers to identifying and establishing leadership, a collaborative planning team, and a list of partners necessary to develop and sustain an information sharing capability. In addition, it is critical to establish trust with traditional and nontraditional groups in advance, define partner roles and responsibilities, and formalize cooperation in the process.

To identify information sharing partners, leaders need to engage in assessments to determine their social and economic profiles. For instance, this process requires a thorough understanding of related jurisdictional risk, vulnerability, and operational requirements to prepare for, respond to, and recover from threats and hazards. Regardless of the governance model, leaders should form a planning team that includes private, NGO, and government partners. Roles may change before, during, and after disasters. The best time to conduct partner engagement is pre-disaster during “blue-sky” periods, but it is appropriate to reach out to build a necessary relationship during a response or recovery.

For example, Wisconsin’s Electrical Utilities – Department of Military Affairs Public-Private Partnership model is a state-led, sector-driven effort. Other jurisdictions have used a partner-managed approach that originated in a planning cell and organized under an Emergency Support Function. The All-Hazards Consortium is an NGO that convenes a national network of organizations to address challenges before, during and after disasters. Furthermore, some P3s establish a virtual or physical BEOC that “facilitates information sharing, coordination and collaboration.” Each model comes with its own legal and ethical considerations, therefore P3 participants should seek to obtain rules of engagement around activities based on local and state laws and existing governance structures.

Getting Started: Illinois Emergency Management Agency

The Illinois Terrorism Taskforce funded the initial development of the P3 to share threat information. The Taskforce made a connection to a private sector liaison in the State Emergency Operations Center to ensure timely and effective operational response coordination. Illinois developed a rolodex of private sector organizations to consolidate P3 efforts. In 2011, this partnership led to the developing of a state BEOC to facilitate all-hazards information sharing.[20]

A P3 should also define the mutual operational information sharing requirements for private sector and public sector partners. What information does each need from the other?

Table 1: Sample Operational Information Requirements

	Public Sector Needs from Private Sector	Private Sector Needs from Public Sector
Resilience	▪ Risk and vulnerability assessments ▪ Industry thresholds, triggers, and targets ▪ Capabilities, assets, and key resources	▪ Resilience strategy and projects ▪ Official situational awareness ▪ Procurement guidance
Response	▪ Business open/closed status ▪ Community lifeline and supply chain status ▪ Resource offers/requests ▪ Impacts to labor ▪ Infrastructure restoration	▪ Declarations/status of operations ▪ Strategic response priorities ▪ Closures/curfews/evacuations ▪ Restrictions/transportation waivers, access/reentry info
Recovery	▪ Estimated time to resume operations/plans to reopen ▪ Economic conditions/housing inventory status ▪ Loss estimates from damages/closures ▪ Resources for donation/mass purchase ▪ Financing options	▪ Economic recovery priorities ▪ Permanent reconstruction plans ▪ Disaster recovery contracts and financing ▪ Support for critical facility restoration ▪ Government assistance

[20] Correspondence with Illinois BEOC leadership. For more information, see https://iema.illinois.gov.

The capability to share the operational information requirements will require thoughtful planning to develop plans and SOPs, technology, training and exercises, and usage considerations. A P3 should identify information sharing use cases, usability requirements and lessons learned from previous after-action reports and improvement planning processes.

During the design process, it is essential to identify planning factors and SOPs related to information access, discovery, retrieval, dissemination, safeguarding, and interoperability. It is also critical to develop information sharing policy guidelines, data and technology standards, information assurance requirements, rules for engagement, and jointly develop operational information requirements.[21] Leaders should consider the role of technology in creating robust information sharing capabilities. Technology includes identifying requirements and establishing plans to utilize technologies. Additionally, this consists of developing and sustaining an information management infrastructure.

Incorporating a plan for training and exercises is another critical component of designing an information sharing capability. In the design phase, identify information sharing capability training and exercise needs and jointly develop operational and technical information sharing capabilities. The next step is developing processes to test plans and evaluation criteria, this may include partnering with existing business alliances and affinity groups that can expand outreach and partner engagement planning efforts with identified partners.[22] Additionally, build on existing partnerships, technologies, and processes to ensure that private and public sector partner use and implement the identified solutions.

2. Implement

A comprehensive information sharing capability requires an organizational structure, operational plans, technical instructions, and technology that supports the exchange of information. Also needed are training and exercises to test and evaluate information sharing capabilities, and an understanding of both how and how often partners use information sharing capabilities.

2.1. Formalize Governance

As information sharing capability development matures, P3s should consider formal charters, membership agreements or information sharing instruments. Organizations should jointly develop and codify all-hazards and incident-specific scenario product templates. **Appendix C:** Sample Information Sharing Agreement serves as an instrument for building trust among partners, enabling them to collaborate effectively without compromising the confidentiality of shared information.

[21] For more information, see https://www.fema.gov/sites/default/files/2020-05/CommunityLifelinesToolkit2.0v2.pdf.

[22] For a list of potential outreach focal points, see https://www.fema.gov/emergency-managers/national-preparedness/plan.

2.2. Jointly Develop Information Sharing Plans and Standard Operation Procedures

The development of information sharing plans and SOPs should establish and facilitate operational information sharing needs and align information sharing plans and SOPs to industry standards,[23] including local, state, regional and national guidance. The plans and SOPs should support joint private and public sector goals. An information sharing plan for a P3 may include components such as the following:

- Inclusion of partners on the P3 distribution list and for daily coordination calls;
- Access to meetings, crisis management platform, and training;
- Description of the P3 incident management system and common operational picture;
- Policies for information discovery, access, and distribution;
- List of common operational data shared;
- Opportunities to participate in assessment, planning and operational decision-making; and
- Business re-entry certification.

The inclusion of private sector information-sharing planning considerations is an essential part of planning. For example, jurisdictions can include private sector considerations in the emergency operations plan EOP base plan, ESF Annex, Recovery Annex, or Threat and Hazard Specific Annex.

Real-world examples include the following:

- EOP Base Plan – North Carolina EOP;[24]
- ESF Annex 14 – Hamilton County, Ohio;[25]
- Private Sector Coordination Support Annex – Illinois Emergency Management Agency;[26]
- State of Oregon ESF 14;[27] and

[23] For more information, see https://emap.org/index.php/what-is-emap/the-emergency-management-standard.

[24] For more information, see https://www.ncdps.gov/our-organization/emergency-management/em-operations/emergency-operations-plan.

[25] For more information, see https://cdnsm5-hosted.civiclive.com/UserFiles/Servers/Server_3788196/File/Government/Departments/EMA/Planning/EOP-Complete-Plan-v.-1.6-Public-Version.pdf.

[26] For more information, see https://iemaohs.illinois.gov/content/dam/soi/en/web/iemaohs/preparedness/documents/ieop/annex-20-private-sector-integration.pdf.

[27] For more information, see https://www.oregon.gov/oem/Documents/OR_EOP_ESF_14_Business_Industry.pdf.

- Pennsylvania ESF 14, Cross-Sector Business and Infrastructure.

> “Private-Public Partnerships in our state support public safety and help protect our economic strength by fostering collaboration, communication, and cooperation, between businesses and the communities they serve. Private sector partners capitalize on shared information to make strong operational decisions, prepare, continue, or resume normal business operations as quickly as possible.”[28]
>
> — N.C. Emergency Operations Plan, 2021

2.3. Establish a Technology Collaboration Environment

The use of information technologies is a force multiplier for collaboration. A mature collaboration environment will clearly describe the following:

- What information is available;
- What services are available;
- What authorizations are required;
- What data standards need to be used;
- The rules under which information is made discoverable and can be shared; and
- How to access or deliver requested information on a predictable and sustainable basis.

[28] Adapted from the North Carolina EOP. Accessible at https://www.ncdps.gov/emergency-operations-plan.

Nebraska Preparedness Partnership

Nebraska Preparedness Partnership (NPP) was formed to build the readiness of private partners in Nebraska to prepare, mitigate, respond, and recover from disasters through advocacy, training and public partnerships. As a nonprofit organization, NPP facilitates sharing information related to preparedness, business continuity strategies and tactics, risk and vulnerability assessment information, training and exercise opportunities and progress reports. Further, the NPP amplifies information from local nonprofit organizations and shares information across regional P3 programs such as the Colorado Emergency Preparedness Partnership and Safeguard Iowa to train and prepare partners.[29]

2.4. Define Test and Evaluation Criteria

The Homeland Security Exercise and Evaluation Program provides a toolkit to support the evaluation of capability targets via exercises. When partners develop exercise plans, they should include criteria to inform observation, data collection, and evaluation of whether and to what extent information sharing is occurring. This is an opportunity to evaluate the use of selected collaboration tools and the implementation of operational workflows and processes. P3s should leverage a training and exercise program to test and evaluate information sharing capabilities across organizations and share relevant, timely, and actionable information and analysis in collaboration with partners. In addition, develop and disseminate effective information products to further strengthen the information sharing capability. Following training and exercise events, partners should engage in after-action meetings or hotwashes to explore what worked well and what requires improvement and decide on a plan of action for executing those improvements.

2.5. Establish Information Sharing Battle Rhythm

The P3 battle rhythm[30] for information sharing should include a phase-based definition of activities, tactics, and cadence for each phase of emergency management. The information sharing battle rhythm should also include touchpoints and alignment with local, state, regional, national, and international partners (as appropriate) in the private and public sectors. The battle rhythm should seek to connect the dots while not making any P3 partner a single chokepoint for communications and information exchange. **Appendix D:** Example Information Sharing Battle Rhythm includes a sample set of battle rhythms for resilience, response, and recovery.

[29] For more information, see https://www.neprep.org/.

[30] For more information on emergency management battle rhythms, see https://www.fema.gov/pdf/emergency/nims/jfo_sop_annexes.pdf.

3. Evaluate

A P3 should routinely assess and refine information sharing capabilities. In addition, review plans and SOPs to ensure ongoing access, coordination, and safeguarding across information classification.[31] Organizations should also evaluate the impacts of technology on achieving operational situational awareness and refine it as appropriate. For evaluation, organizations should routinely update plans and SOPs that govern information discovery, access and distribution based on lessons learned during exercises. Initiate planning to test and evaluate.

The P3 Information Sharing Functional Model provides an assessment framework that defines the core elements, key functions, and tasks. This model provides a process to measure and report the use and usability of information sharing systems during planned events and incidents.

Table 2: Sample Data Collection and Information Sharing Objectives

Resilience	Response and Recovery
▪ Obtain risk and vulnerability assessment data ▪ Conduct and share risk and vulnerability assessment information ▪ Ensure data quality ▪ Advertise training and exercise opportunities ▪ Coordination across regional P3 programs ▪ Advocacy in trade associations ▪ Promote business continuity strategies and tactics ▪ Marketing and outreach materials, presentations, web presence ▪ Provide preparedness information ▪ Program progress reports and newsletter	▪ Obtain sector-specific and economic impact assessments ▪ Gather and share operational status information ▪ Joint prioritization and sequence of response and recovery missions ▪ Provide incident-specific or event-specific situation reports ▪ Use of designated crisis management system ▪ Expand the P3 common operating picture ▪ Coordination of needs and resources ▪ Foster cross-sector problem solving ▪ Removal of functional barriers to private sector response and recovery missions ▪ Business re-entry and resumption of normal operations as soon as possible

Organizations may also request support from the National Council of Information Sharing and Analysis Centers, which helps jurisdictions reduce cyber risks and build resilience.[32] A mature information sharing capability will produce results that achieve the objectives described in this guide.

[31] For this guide, classification examples include: Open Source, Business Confidential, Sensitive but Unclassified, For Official Use Only, Secret and Top Secret.

[32] For more information, see https://www.fema.gov/emergency-managers/national-preparedness/plan.

Appendix A: Functional Information Sharing Model

The Functional Information Sharing Model provides a roadmap to support the development of a comprehensive information sharing capability for a P3.[33]

Table 3: Functional Information Sharing Model Overview

Core Elements	Design	Implement	Evaluate
Governance	Establish leadership for information sharing capabilities	Jointly develop information sharing capabilities	Routinely assess and refine information sharing capabilities
Planning and SOPs	Develop guidelines, and operational information requirements	Jointly develop information sharing plans and standard operating procedures	Review safeguarding across information classification domains
Technology	Identify technology requirements	Establish a secure collaboration platform	Evaluate achieving operational situational awareness
Training and Exercises	Develop training and exercises to test and evaluate information sharing capabilities	Test and evaluate information sharing capabilities across organizations	Routinely update plans and SOPs
Usage	Identify usability requirements for information sharing	Share actionable information and analysis and develop and disseminate helpful information products	Measure use and usability of information sharing systems and processes

[33] The Functional Information Sharing Model is adapted from the strategic P3 Information-Sharing Continuum in the Building Private Public Partnerships guide.

1. Functional Information Sharing Model Definitions

1.1. Core Element 1: Governance

Governance includes the legal, policy and organizational structure and processes supporting decision-making, accountability, control, and behaviors. Effective governance also includes transparency, ensuring that relevant information and processes are accessible and visible to partners. This transparency further empowers partners to collaborate and make well-informed decisions that mutually benefit their organizations and the communities they serve.

1.2. Core Element 2: Planning and Standard Operating Procedures

Plans and SOPs are those formal written operational and technical guidelines or instructions for information management within and across organizations. Good planning will offer partners a specific plan and clear procedures ensuring a standardized approach to information sharing, utilization, and degraded communications.

1.3. Core Element 3: Technology

Technology may include any mode of exchanging information such as email, phone, text, listserv, social media, website, email distribution list, web conference platform or information exchange platform (e.g., Microsoft Teams, ArcGIS, WebEOC). Good technology superimposes the human and organizational intent into a functional tool or template.

1.4. Core Element 4: Training and Exercises

Training and Exercises include developing training and exercises to test and evaluate information sharing capabilities to ensure that the operational and technical components function as designed. Good training and exercises include functional tests and evaluation of information sharing capabilities that enable seamless response and recovery operations and support building resilience.

1.5. Core Element 5: Usage

Usage refers to how often partners use information sharing capabilities. It also refers to the effectiveness of configuring capabilities to support usability and workload requirements. Usage also addresses how private and public sector partners routinely use effective information management systems, which will make their job easier.

Appendix B: Information Sharing Assessment Tool

This appendix provides a self-assessment tool that enables partners to assess readiness to share information during all phases of emergency management.

1. Information Sharing Assessment Tool

How to use this worksheet: Tally your score to see where you stand.

At every level, each "not yet" statement is worth 0 points, each "in progress" statement is worth 1 point and each "complete" statement at the basic maturity level is worth 2 points. The maximum number of points is 30.

Score of 0-10: You are at or near a basic level of maturity. The good news is you can use our resources now and no-cost solutions to assist you.

Score of 11-20: You are at an intermediate level of maturity and have taken some meaningful steps toward the development of a P3 information sharing capability. There is room to improve.

Score of 21-30: You are at an advanced level of maturity and are further along in your P3 information sharing. There are some steps you can take to improve.

2. Governance – Design

Establish leadership necessary to develop and sustain an information sharing capability.

Not yet	In progress	Complete

3. Plans and Standard Operating Procedures – Design

Develop information sharing policy guidelines, data and technology standards, rules for engagement and jointly develop operational information requirements.

Not yet	In progress	Complete

4. Technology – Design

Identify technology needs and requirements, utilize existing technologies or develop and sustain information management infrastructure. (Note: This can include identifying communities where sharing information via existing technologies may be challenging).

Not yet	In progress	Complete

5. Training and Exercises – Design

Identify information sharing training and exercise needs and test plans and evaluation criteria.

Not yet	In progress	Complete

6. Usage – Design

Identify information sharing use cases, usability requirements and lessons learned from previous after-action reports and improvement planning processes.

Not yet	In progress	Complete

7. Governance – Implement

Jointly develop private-public information products for all-hazards and incident-specific scenarios.

Not yet	In progress	Complete

8. Plans and Standard Operating Procedures – Implement

Jointly develop information sharing plans and standard operating procedures. Align information sharing plans and SOPs to industry guidance and local, state, regional and national guidance.

Not yet	In progress	Complete

10. Technology – Implement

Setup and maintain a collaboration platform and other primary and alternate methods of communication to facilitate ongoing collaboration between stakeholder groups.

Not yet	In progress	Complete

11. Training and Exercises – Implement

Deliberately test and evaluate information sharing capabilities across organizations.

Not yet	In progress	Complete

12. Usage – Implement

Share relevant, timely and actionable information and analysis in collaboration with partners and develop and disseminate useful information products.

Not yet	In progress	Complete

13. Governance – Evaluate

Routinely assess and refine information sharing capabilities.

Not yet	In progress	Complete

14. Plans and Standard Operating Procedures – Evaluate

Review ongoing access, coordination and safeguarding across information classification domains (Open Source, Official Use Only, Unclassified, Classified).

Not yet	In progress	Complete

15. Technology – Evaluate

Evaluate impacts of technology on achieving operational situational awareness, assess how information is being delivered via alternate means, and refine as appropriate.

Not yet	In progress	Complete

16. Training and Exercises – Evaluate

Routinely update plans and SOPS that govern information discovery, access and distribution based on lessons learned.

Not yet	In progress	Complete

17. Usage – Evaluate

Measure and report on the actual use and usability of information sharing systems and processes. Routinely conduct information sharing after-action reports and improvement plans.

Not yet	In progress	Complete

Appendix C: Sample Information Sharing Agreement

The sample Information Sharing Agreement serves as an instrument for building trust among partners, enabling them to collaborate effectively without compromising the confidentiality of shared information. The agreement provides a framework to harness the mutual benefits of shared knowledge while upholding ethical and legal standards. This sample agreement is adapted from an archived Department of Homeland Security (DHS) Virtual USA Information Sharing Agreement.

1. Article I - Purpose and Authorities

This memorandum of agreement (MOA) is made and entered into by and between participating partners, which enact this agreement, hereinafter called Members. The purpose of this MOA is to provide a governance framework for information sharing between the Members entering this MOA and any Member designee, herein referred to as an authorized representative who participates in the information sharing or consumption of said information.

2. Article II - General Implementation

The prompt, full and effective use of shared information among participating Members, including any information on hand or available from participating partners or any other source, which are essential to the safety, care, and welfare of the people in the event of any incident affecting a party Member, shall be the underlying principle on which all articles of this MOA shall be understood.

Each party Member entering this MOA recognizes the following:

- Many incidents transcend jurisdictional boundaries;
- Intergovernmental information sharing and coordination is essential in managing these and other incidents under this agreement;
- There will be incidents which require immediate access to information in another jurisdiction;
- Sharing information during incidents is critical to other Members' prevention, protection, response, and recovery efforts; and
- There is a need for information to be timely and accurate.

On behalf of the authorizing body for each Member participating in the agreement, the authorized representative who is assigned responsibility for incident management will be responsible for formulation of the appropriate multi-jurisdictional prevention, protection, response, and recovery procedures necessary to implement this MOA.

3. Article III - Party Member Responsibilities

It shall be the responsibility of each party Member to formulate internal procedural plans and programs for multi-jurisdictional resilience and all response and recovery efforts that support the performance of the responsibilities listed in this article. In formulating such plans,

and in carrying them out, the party Members, as far as practical, shall acquire and develop information sharing capabilities that best meet their needs and maintain reliable data sources.

A Member's authorized representative may request assistance of another Member's authorized representative by contacting them directly. The provisions of this agreement shall only apply to requests for information made by and to authorized representatives. Requests may be verbal or in writing. If verbal, the request shall be confirmed in writing within 30 days of the verbal request. Requests shall provide a description of the information request and the point of contact.

4. Article IV - Information Requirements

Information Sharing: Party Members agree to pre-identified types or categories of data layers to share from a pre-identified list of priority data sources as needed and as noted in the MOA appendices. Members agree that all information will only be shared using the information sharing structure described in Article V and no copies of the source data will be posted or distributed in any form.

Information Assurance: Each Member will provide information assurance to verify that all shared data are derived from an authoritative data source (custodial owner). Members shall not directly contact another Member's data source but will agree to work with the data coordinator (Member) for any follow-up required from the information provided. Members, as far as practical, will provide data layers with the metadata requirements identified in the MOA appendices.

Requests for Information: Members, as far as practical, agree to automate requests for information and handle such transactions between relevant members on a case-by-case basis.

5. Article V - Architecture

Members will be responsible to develop their respective internal information sharing architectures needed to support information sharing between disparate Member visualization tools. Members will, within their respective architectures, identify and solve technical challenges that hinder or prevent the necessary sharing of information. At a minimum, Members agree upon an information sharing structure, how to share data files and analytical services, cybersecurity requirements and information protection standards for all participants as outlined hereafter.

Information Sharing Structure: Insofar as practical, Members shall agree to share information directly with other Members based on the terms outlined in this MOA and/or provide access to each of their available data layers through the information sharing structure described in the MOA appendices. Members will share information by granting access to the relevant data layer streams from their servers to other Members.

Data Files and Analytical Services: Insofar as practical, Members agree to use open-source standards and publish their data files in the pre-identified data file extensions identified in the MOA appendices. Each party will work toward producing a web service so that all Members may consume the information using a technology agnostic platform if technically feasible.

Cybersecurity: Participants will adhere to baseline system security requirements for information to be shared across all jurisdictions. Member system security protocols will adhere to standard industry best practices.

Identity Management: Members will vet users through their own internal process wherein Member's' information coordinators will sponsor individual participation and third-party access to information. Only Members' information coordinators will have access to the information sharing structure.

Information Protection: Members will agree to only share information in accordance with its classification including Protected Critical Infrastructure Information and law enforcement sensitive information. Members will agree to the roles and levels of security and data sensitivity that are used in the information sharing structure identified in the MOA appendices.

6. Article VI - Permissions to Share

Due to the sensitive nature of information shared relative to a multi-jurisdictional incident, Members agree to adhere to information sharing permissions, to the extent permitted by Members' freedom of information laws. Members must obtain the permission of the data provider prior to sharing information with non-Members and only use information for the authorized purposes under this agreement. This may be performed on a case-by-case basis or through a memorandum of understanding.

7. Article VII - Liability

Officers or employees of party Members rendering support or technical assistance to another Member pursuant to this MOA shall be considered agents of the requesting Member for tort liability and immunity purposes; and no party Member or its officers or employees rendering support or assistance to another Member pursuant to this MOA shall be liable on account of any act or omission in good faith on the part of such forces while so engaged. Good faith in this article shall not include willful misconduct, gross negligence, or recklessness.

Members will use any information or technical assistance provided by other Members at their own risk. Inasmuch as Members adhere to the information assurance process, no Members shall hold others liable and all Members acting in good faith will be indemnified from any liability claims to the extent permitted by the Member's' laws, assuming also that the source will be responsible for the quality, accuracy and scoring of their data.

8. Article VIII - Implementation

This MOA shall become operative immediately upon its endorsement by any two (2) Members; thereafter, this MOA shall become effective as to any other Member upon its endorsement. This document is for the sole benefit of the signatory parties, and no third party is intended to be a beneficiary thereof or have any rights because of this document. Any party Member may withdraw from this MOA, but no such withdrawal shall take effect until 30 days after the authorized representative of the withdrawing state has given notice in writing of such withdrawal to all other party Members. Such action shall not relieve the withdrawing Member from provisions assumed hereunder prior to the effective date of withdrawal.

Duly authenticated copies of this MOA and of such supplementary agreements as may be entered into shall, at the time of their approval, be deposited with each of the party Members.

9. Article IX - Validity

This MOA shall be construed to effectuate the purposes stated in Article I hereof. If any provision of this MOA is declared unconstitutional, or the applicability thereof to any person or circumstances is held invalid, the constitutionality of the remainder of this MOA and the applicability thereof to other persons and circumstances shall not be affected thereby.

Signature Date

Title Jurisdiction/Organization

Effective Date Expiration Date

Appendix D: Example Information Sharing Battle Rhythm

For any private-public partnership (P3), the resilience (preparedness and mitigation) battle rhythm might include the following:

- **Initial messaging to partners.** This may include information about membership, memoranda of agreement, onboarding, system registration and access and capability assessment.
- **Monthly messaging to partners.** This may include general P3 program or business emergency operations center (BEOC) updates and information about trainings, exercises, conferences, opportunities to serve on a task force, amplification of federal messaging, warnings (i.e., cybersecurity updates) and planning updates.
- **Quarterly P3 Program Reviews.** This may include a progress review, briefing on essential policy updates, working group progress reports and advertisement for upcoming training, drills, and exercise opportunities.
- **Seasonal Reports.** This may include hazard-specific preparedness information, and business continuity recommendations. It may also include touchpoint preparation meetings (e.g., pre-hurricane and winter meetings to check readiness, limitations and needs).
- **Annual Reports.** This may include after-action and improvement plan reports, assessment reports, updated social and economic profiles, annual meeting reports, P3 mitigation priorities and other significant information products.
- **Ad hoc Information.** This may include presentations, social media, lessons learned documents and major publications such as an EOP, Private Sector Coordination Annex, continuity of operations plan, etc. It may also include updates on the status of corrective actions.
- **Requests for Information.** This may include pre-registration for access/re-entry programs, completing P3 membership applications, business and industry capability and readiness assessments, P3 mitigation project proposals for the Building Resilient Infrastructure and Communities program.
- **Exercise Discussions.** This may include better understanding of the operational environment and information needs among P3 partners through exercise discussions.

The response and recovery battle rhythm might include the following:

- **Pre-activation information exchange with partners.** This may include the following:
  - Advance notice incident alerts and notifications, an invitation to virtual briefings, direction to P3 members to prepare deployable assets, coordination to pre-position crews and force packages and requests for staging support;

  - Reminders to log in, monitor and populate the crisis management platform, on-the-fly registration information, role assignments, completion of administrative documentation; and
  - Invitations to work at a BEOC/emergency operations center (EOC) or lead a work stream.
- **Activation information exchange with partners.** This may include the following:
  - Daily live operational briefs (in-person and virtual) at the EOC every eight hours, daily briefings at a set time, status updates, sector analysis, capabilities and limitations, operations concerns, future planning considerations and announcements;
  - Status updates two to three times daily pertaining to declaration status, executive orders, transportation waivers, updates to weather, situation reports, executive summaries, road closures, critical infrastructure and community lifelines and amplification of private and public sector messaging at all levels, use of crisis management system to communicate real-time changes such as business open/closed status;
  - Coordination of resource requests, allocations, status (in progress, enroute, on scene, complete); coordination of private sector offers of assistance and delivery of donations; coordination with the public information officer and joint information center regarding public donations; business-to-business mutual aid; coordination of re-entry operations with law enforcement; and
  - Task force organization and communications to support on-the-fly problem solving.
- **De-activation information exchange with partners.** This may include the following:
  - Final operational call. After-action review/hotwash to include successes, challenges, proposed improvements, solutions, and recommendations;
  - Final coordination of resource requests and demobilization of assets; and
  - Final briefing to respective private and public sector EOCs, including public and private sector analyses, identification of strategies to support recovery and coordination with insurance industry partners.
- **Recovery information exchange with partners.** This may include the following:
  - Coordinate re-entry requirements, permits and waivers;
  - P3 partners provide feedback via in-person, by webinar or electronic survey;
  - Recovery notices such as an operational shift to the Joint Field Office, communications to support individual assistance, identification of unmet needs, advertisement of housing forums and just-in-time workshops for underutilized/underserved businesses;
  - Joint survey to all associations, chambers of commerce and businesses for damage and recovery assessments. Coordination of community recovery needs and requirements for donations;
  - Recovery task force briefings focused on business and workforce development focused and on temporary housing; and
  - Lessons learned/after action reviews.