noggin

Emergency

Guide to Achieving Interoperability in Information and Emergency Management

First, why interagency cooperation matters

Few things are more challenging for responder agencies than procuring and deploying the right resources during a large-scale emergency. Already difficult, emergency incident response taxes oft-scarce resources, be they personnel, skills, technologies, facilities, equipment, or funding. And those resources matter. They matter a lot. During an emergency, getting the right resources to the right place at the right time often proves the difference between life or death.

So, what's to be done? For one, interagency cooperation can effectively buoy the response effort. As a collective, cooperating partner agencies can achieve more than any one agency acting on its own. By pooling resources, agencies can amplify resource development and deployment.

Field research bears this out. Effective interagency cooperation creates a positive feedback loop. The right services and programs get recognition and visibility, which, in turn, provides more opportunity for vital, new projects to be undertaken[i].

The right services & programs get recognition & visibility, which, in turn, provides more opportunity for vital, new projects to be undertaken[i]

But interagency cooperation doesn't happen easily. It takes hard work and planning, because the challenges are so stark. For instance, in this era of emergency IT solutions, the ability of responders from different agencies to work seamlessly with other systems or products is becoming an ever-larger component of interoperability. More than ever, responders need to be able to talk to each other and share information on demand and in real time. Using interoperable technologies helps facilitate more efficient communication as well as lets agencies deploy the best resources into the disaster zone, mitigating catastrophe in the process.

Of course, interoperability isn't only beneficial during the actual emergency response. Agencies who incorporate interoperability into planning for major events or even business-as-usual activities, for instance, can also maximize resources, giving themselves a substantial head start in case a disaster actually strikes. The question remains, though, how?

At a glance: The challenges of interagency cooperation

Achieving comprehensive interoperability between multiple stakeholder agencies, often working across jurisdictional and/or regional lines, takes effort. Responder agencies in both the public and non-governmental sectors will often have to contend with limited or fragmented sources of funding. Finance and procurement teams might be hesitant to devote scarce resources to working better with other agencies.

What's more, agencies often don't think they need to prioritize interoperability. It's not uncommon that agencies will only perceive the crucial need after an incident unfolds, by which time it's already too late to put interagency protocols in place.

While those human and financial factors are significant, they aren't the only challenges to achieving interoperability. Other challenges include:

Planning. As mentioned, interoperability starts with planning. Agencies must identify roles and responsibilities for personnel dealing with unexpected incidents. Those plans should lay out how specific agency personnel will work in coordination with responders at partner agencies.

Training. Planning is only the first step. Agencies need to bring those plans to life by training their personnel (often alongside partners) on roles and responsibilities.

That's difficult when senior stakeholders are too busy to train personnel, or don't have the interoperability experience themselves to make trainings effective. Additionally, roping in partner organizations to participate in trainings might prove logistically difficult.

Technology. Of course, agencies can have the best intentions of achieving interoperability. But if they don't have the right tools to enable interagency cooperation, little will get accomplished.

By in large, there's an industry-wide need for better technology to support interagency (and intra-agency) collaboration and communication during emergency response. For instance, responders often complain of information-overload during emergency response, because they don't have the right electronic messaging tools.

Here again, agencies working with limited financing won't necessarily have the budgets to procure the right technologies, or upgrade aging equipment. Moreover, even those teams who purchase next-gen technologies might find that those services aren't always compatible with a partner agency's solution stack.

Understanding interoperability frameworks: the case of the Incident Command System

The necessity of interagency cooperation hasn't been lost on the emergency management community who has, in turn, built frameworks to enable interoperability in all aspects of incident management. Created in response to a breakdown of interagency cooperation, the operational incident management structure, Incident Command System (ICS), for one, provides a standardized approach to the command, control, and coordination of emergency response for organizations across the U.S.

At its core, ICS is meant to enable the effective and efficient management of incidents, irrespective of jurisdiction, kind, complexity, or size. The system codifies emergency management best practices into a unified approach to incident response, integrating a combination of facilities, equipment, personnel, procedures, and communications, which then all operate under a common organizational structure.

One of the reasons ICS has proven so successful at facilitating interoperability and interagency cooperation on the ground is because it offers this common incident management vocabulary for all organizations involved in incident response. As a result, personnel from multiple agencies can communicate using the same language, rather than their own agency-specific terminology, an oft-cited barrier to interagency cooperation. The system thus lets incident managers set up a unified, centrally authorized, emergency command structure quickly, without fear of miscommunication in the field or in the incident command center[ii].

The system thus lets incident managers set up a unified, centrally authorized, emergency command structure quickly, without fear of miscommunication in the field or in the incident command center[ii]

Nor are flexibility and standardization the system's sole attributes. ICS creators developed the system with 14 core features in mind. Those features fall into the following types: standardization, command, planning structure, facilities and resources, communications and information management, as well as professionalism. The features are described in Table 1 on page 4.

How, exactly, can ICS bolster your interagency information and incident management efforts? A FEMA position paper puts this best: "There will be instances in which successful domestic incident management operations depend on the involvement of emergency responders from multiple jurisdictions, as well as personnel and equipment from other states and the federal government. These instances require effective and efficient coordination across a broad spectrum of organizations and activities"[iii].

These instances require effective & efficient coordination across a broad spectrum of organizations & activities[iii]

And that's where ICS proves of greatest value. The system facilitates the easy mobilization of outside resources, designed as it is so that everyone knows what's going on. But the system doesn't just come in handy during an incident. It also helps organizations unite, plan, and simulate their responses before the incident breaks out in the first place.

ICS also provides a rich stockpile of best practices. Having experienced some of the ruinous effects of inadequate joint planning up close, ICS creators took the imperatives of coordinated planning very much to heart. And that's why, ICS, as it stands today, offers a pretty thorough process for incident planning, culminating in the development of the Incident Action Plan (IAP).

The IAP documents incident goals, objectives, and strategies, as well as contains tactics and vital information for managers and responders. Far from a static document, the IAP is meant to evolve as incident parameters change and facts on the ground shift, thereby giving agencies an important means by which to disseminate critical information before, during, and after the incident[iv].

Table 1. Incident Command System (ICS)

Type	Feature	Purpose
Standardization	Common terminology	Helps define organizational functions, incidents facilities, resource descriptions, and position titles.
	Establishment and Transfer of command	Command must be clearly established from the outset of the incident. Command must be transferred only with a briefing that captures all essential information for continuing safe and effective operations.
	Establishment and Transfer of command	Command must be clearly established from the outset of the incident. Command must be transferred only with a briefing that captures all essential information for continuing safe and effective operations.
	Unified command	Enables agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively under individual agency authority, responsibility, or accountability.
	Management by objectives	Includes establishing overarching objectives; developing strategies based on incident objectives; developing and issuing assignments, plans, procedures, and protocols; establishing specific, measurable objectives for various incident management functional activities and directing efforts to attain them, in support of defined strategies; and documenting results to measure performance and facilitate corrective action.
Planning and organizational structure	Modular organization	The organizational structure is based on the size and complexity of the incident, as well as the specifics of the hazard environment created by the incident.
	Incident action planning	Offers a coherent means of communicating the overall incident objectives in the context of both operational and support activities.
	Manageable span of control	Span of control of any one individual should range from three to seven subordinates.
	Incident locations and facilities	Operational support facilities will be established in the vicinity of an incident, e.g. incident command posts, bases, camps, staging areas, mass casualty triage areas, etc.
Facilities and resources	Comprehensive resource management	Stipulates accurate, up-to-date accounting of resource use.
	Integrated communications	Develop and use a common (incident) communications plan and interoperable communications, processes, and structures.
Communications and Information Management	Information and Intelligence management	Establish a process for gathering, analyzing, sharing, and managing incident-related information and intelligence.
	Accountability	Effective accountability is considered essential during incident operations. As such, the following principles must be adhered to: • Check-in • Incident Action Plan • Unity of command • Personal responsibility • Span of control • Real-time resource tracking
Professionalism	Dispatch/deployment	Personnel and equipment should only respond when requested or when dispatched by the appropriate authority.

ICS and the National Incident Management System (NIMS)

ICS surged in popularity as soon as it was developed – adopted to use cases far beyond the fire suppression context and replicated across the globe (see, for example: the Austral-asian Inter-service Incident Management System). No doubt, one of the most important milestones in this trajectory was the decision to include ICS as a key feature of the U.S. National Incident Management System (NIMS), when that system was created in the 2000s. In fact, we might say that single decision helped spur greater (non-fire) adoption of ICS than anything else.

Put out by the U.S. Department of Homeland Security, NIMS lays out a standardized approach for tackling all-hazard situations, offering a consistent nationwide approach for federal, state, tribal, and local governments to use when working together to prepare for, prevent, respond to, and recover from domestic incidents of any cause, size, or complexity.

Like ICS, NIMS incorporates existing best practices-after all, it was developed after close collaboration between state and local government officials and representatives from a wide range of public safety organizations-into a comprehensive national approach to incident management. The approach taken by NIMS is based on a few core concepts, not too dissimilar to ICS':

A consistent method for identifying, acquiring, allocating, and tracking resources

Standardized systems for classifying resources to improve the effectiveness of mutual aid assistance agreements

Coordination to facilitate the integration of resources for mutual benefit

Use of all available resources from all levels of government, nongovernmental organizations, and the private sector, where appropriate

The integration of communications and information management elements into organizations, processes, technologies, and decision support

The use of credentialing criteria that ensures consistent training, licensing, and certification standards

NIMS essentially boils down to proper planning before an incident, during which time organizations should inventory and categorize their resources by kind and type, including size, capacity, capability, and other characteristics.

Source: U.S. Department of Homeland Security

Examples of successful interagency cooperation

Interagency frameworks and systems like ICS have gone a long way towards mitigating key interoperability challenges, such as an uptick in natural disasters and the fact that relief agencies have historically developed along parallel tracks. But how have those frameworks and systems performed on the ground?

As responder agencies have begun to prioritize interoperability, we're starting to see more examples of effective interagency cooperation in the incident management space. Here are a few notable instances:

11 September.
Though generally considered a failure of interoperability, the emergency response to the 11 September terrorist attacks wasn't without moments of sterling interagency cooperation. For instance, nearly one thousand responders from 50 agencies communicated effectively in the response to the Pentagon crash of American Airlines Flight 77.

Here, responder agencies had internalized the lessons of the Air Florida crash of the early 1980s, when a plane crashed into a Washington, D.C. bridge during a snowstorm. Though emergency responders arrived at the scene quickly, the effort was hampered and delayed, because agencies couldn't communicate with each other quickly[v].

Cyclone Debbie.
Cyclone Debbie was one of the most powerful storms to hit Australia in the last decade, causing widespread damage and leading to the loss of 14 lives. In the storm's destructive wake, the state of Queensland ordered a full investigation into the effectiveness of the disaster response.

The report was published in late 2017. And when it came to interoperability in information management, the report cited a generalized lack of awareness of how various systems worked together and exchanged information. That lack of awareness stymied the efforts of multi-agency operators to use those systems effectively[vi].

There were bright spots though. The event management system, built by integrated safety and security management software company, Noggin, actually made a strong debut during the Debbie response. As the report writers detail:

From a systems perspective, we heard these were a great improvement from previous event reporting methods. We heard positive feedback about the [event management] system, including that it was easy to use, reliable because information could be updated as changes occurred, and accessible, as it could be used remotely and those on duty did not have to be in the SDCC [State Disaster Coordination Centre] to update their information. We heard positive feedback about the reports, in particular that the level of detail included was useful[vii].

2018 Commonwealth Games. As mentioned, emergency response isn't the only scenario that stands to benefit from interagency coordination. Preparing for global summits and international sporting spectacles, mega-events like the G-7 or World Cup, also demand a high degree of multi-agency interdependency. Queensland security officials found themselves in that situation after the city of Gold Coast was selected to host the 2018 Commonwealth Games.

Since there wasn't already an interoperable framework for safety and security during mega-events, officials had to build a multi-tiered structure. First, they tasked the games' organizers with facilitating venue and event security. Just above that rung, the Queensland Police Service (QPS) would provide a security overlay. And finally, the Australian federal government, specifically the Attorney's-General Department, would take care of crisis management and matters of national security.

The QPS had a lot to consider. For one, the agency is integrated into the information management structure, the Joint Intelligence Group (JIG). Integrated in the JIG, as it is, the QPS also had to share information across multiple security agencies. Fortunately, QPS was prepared. The Noggin incident management system was already the group's platform for information management tasking during the Brisbane G20 in 2014.

> The result: from the baton relay to the closing ceremony of the Commonwealth Games, the QPS was able to use the Noggin system, rebranded as the Queensland Intelligence and Tasking System (QITS,) to great effect. Specifically, the QPS registered record usage on the system for the length of the games. The large volume of data input enabled a common operational picture to emerge. All in all, the solution gave the QPS and other agencies better situational awareness, furnished a common operation picture, and even helped formalize new communication flows.

If the examples cited are any indication, two things are true: interoperability is possible, and its benefits are manifold. As such, the onus is on first responders, emergency managers, government agencies, and non-governmental, public safety organizations to transition to interoperable systems, so as to enable effective interagency cooperation, either in the event of a largescale emergency, a major event, or more day-to-day emergency situations.

What will it take: finding solutions, like Noggin Emergency, that give agencies the information and tools that they need to effectively manage all emergencies, through the entire lifecycle of preparation, response, and recovery, as well as business-as-usual operations for emergency preparedness and critical infrastructure. Specifically, accelerating coordinated decision making and improving response outcomes takes access to best-practice libraries, incorporating content from interoperable frameworks like ICS, of pre-configured, best-practice incident templates, dashboards, and especially ICS forms and reports, like ICS 214, ICS220, ICS204, ICS205A, etc.

Citations

i Kimberley I. Shoaf, Melissa M. Kelley, et al., Public Health Reports: Enhancing Emergency Preparedness and Response Systems: Correlates of Collaboration Between Local Health Departments and School Districts. Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4187313/.

ii Federal Emergency Management Agency: NIMS and the Incident Command System. Available at https://www.fema.gov/txt/nims/nims_ics_position_paper.txt.

iii Ibid.

iv U.S. Department of Health & Human Services: Office of the Assistant Secretary for Preparedness and Response: What Is An Incident Action Plan? Available at https://www.phe.gov/Preparedness/planning/mscc/handbook/Pages/appendixc.aspx.

v Federal Emergency Management Agency: National Incident Management System (NIMS), An Introduction. Available at https://emilms.fema.gov/IS700aNEW/NIMS01summary.htm.

vi Inspector-General Emergency Management. The Cyclone Debbie Review: Lessons for delivering value and confidence through trust and empowerment. Available at https://www.igem.qld.gov.au/reports-and-publications/Documents/Cyclone%20Debbie%20Review%20Rpt1-17-18_PUBLIC_WEB.pdf.

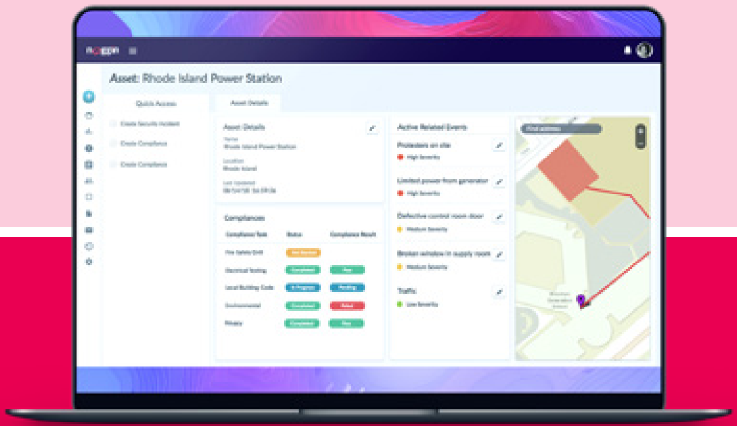
vii Ibid.

Like what you read?
Follow Noggin on social media

@teamnoggin

facebook.com/teamnoggin

linkedin.com/company/noggin-it



Asset: Rhode Island Power Station

noggin
for Emergency

Keep your organization secure and operating smoothly, using the world's leading platform for integrated safety and security management. Enhancing the benefits of a Noggin solution pack, Noggin for Emergency provides you all the information and tools that you need to effectively manage safety, security, business disruption, and business continuity, from the smallest incident or service outage to a major crisis.

The Noggin for Emergency industry pack provides access to the Noggin Library of best-practice templates, forms, dashboards, and more.

To learn more,
visit: **www.noggin.io**
or contact: **sales@noggin.io**