Before the
Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Washington, DC 20528

In the Matter of	)	
	)	
Incident Communications Activity Report	)	CISA-2022-0012
	)	

COMMENTS

CTIA[1] respectfully responds to the *Request for Comments* ("*RFC*")[2] issued by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") Emergency Communications Division ("ECD") in the above-captioned proceeding. The *RFC* proposes to collect information from ECD stakeholders, including state and local emergency communications professionals, regarding any organized incident management command and coordination structure established for an incident, planned event, or exercise.

The wireless industry appreciates CISA's efforts to enhance the resilience of public safety communications capabilities by providing technical assistance and sharing best practices with National Security and Emergency Preparedness stakeholders, including state and local emergency response officials. CISA should ensure that Incident Communications Activity Reports are focused on "public safety communications technologies" controlled by reporting

[1] CTIA —The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers, as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Incident Communications Activity Report, 87 Fed. Reg. 63792 (rel. Oct. 20, 2022) ("*Request for Comment*").

state or local emergency response officials, as the Federal Communications Commission ("FCC") already collects and shares with CISA information about the availability of commercial communications services related to disaster events. If information about commercial communications services is collected in Incident Communications Activity Reports, CISA should direct that reporting state and local public safety officials coordinate with relevant commercial providers and treat such information as confidential.

I. INTRODUCTION AND SUMMARY.

The wireless industry shares the mission of CISA's ECD to promote communications used by emergency responders and government officials to keep America safe, secure, and resilient. For years, the wireless industry's voluntary Wireless Network Resiliency Cooperative Framework ("Framework") has successfully enhanced the availability of mobile wireless services during disaster events through investment, preparation, and coordination.[3] CTIA also helped launch the Cross-Sector Resiliency Forum to enhance resiliency coordination and collaboration among industry sectors, including electric power companies.

Recently, the FCC recognized the Framework's "commendable eight-year track record" and adopted new rules to extend the Framework to all facilities-based wireless providers.[4] These new rules include an obligation on wireless providers to submit "after-action" reports to the FCC that describe how the Mandatory Disaster Response Initiative ("MDRI") provisions

[3] CTIA, *Preparing for Emergencies*, https://prepared.ctia.org/ (last visited Dec. 19, 2022); *The Wireless Industry Responds to 2022 Hurricane Season*, CTIA Blog (Sept. 28, 2022), https://www.ctia.org/news/the-wireless-industry-responds-to-2022-hurricane-season.

[4] *See Resilient Networks; Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications; New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Report and Order and Further Notice of Proposed Rulemaking, FCC 22-50 ¶ 15, App. A at 47 C.F.R. § 4.17 (rel. July 6, 2022) ("*Resilient Networks Order*").

facilitated resiliency for a particular disaster event.[5] The FCC also collects information on the status of commercial communications services during disasters and emergencies, and shares this data with CISA, among others, through the Disaster Information Reporting System ("DIRS").[6]

In this proceeding, CISA should ensure that Incident Communications Activity Reports do not duplicate these efforts. Specifically, CISA should ensure that Incident Communications Activity Reports focus on "public safety communications technologies" controlled by reporting state or local emergency response officials.[7] The resilience of public safety communications technologies during a disaster event is relevant to CISA and, just as importantly, reporting public safety officials have direct knowledge to contribute. To the extent Incident Communications Activity Reports seek information about commercial communications services, CISA should direct reporting state and local officials to coordinate with commercial providers to ensure that the reported information is accurate. CISA should also treat information about commercial communications services as confidential.

II. THE WIRELESS INDUSTRY IS IMPROVING NETWORK RESILIENCY AND RESTORATION THROUGH INVESTMENT AND PREPARATION.

For years, the Framework has successfully enhanced network resiliency through investment, preparation, and coordination with a particular focus on roaming, mutual aid, and public safety and consumer preparedness. Hurricane Ian is the latest disaster event that demonstrates the value of investment, preparation, and collaboration through the Framework. In spite of the massively powerful Category 4 storm, the vast majority of consumers in Florida and

[5] *Id*. ¶¶ 32-34.

[6] *See* Federal Communications Commission, *Disaster Information Reporting System (DIRS)* (updated Aug. 29, 2021), https://www.fcc.gov/general/disaster-information-reporting-system-dirs-0.

[7] *Request for Comment*, 87 Fed. Reg. at 63793.

South Carolina were able to maintain vital connections throughout the storm. For example, 89% of the more than 14,000 cell sites in Ian's path stood up to the hurricane's extreme winds and flooding, improving to 94% within one day after Hurricane Ian passed through Florida. And where Hurricane Ian decimated local infrastructure—bridges, buildings, and power grids—the wireless industry was able to keep more than 12,600 cell sites operational, including more than 500 cell sites running on backup power. [8]

Recognizing the success of the Framework among the voluntarily participating wireless providers, the FCC recently adopted new rules to extend the Framework to all facilities-based wireless providers to engage in roaming under disaster ("RuD"), mutual aid, and other preparedness activities related to a disaster event. Notably, the FCC's new MDRI also compels wireless providers to submit "after-action" reports that describe how the MDRI provisions were implemented by wireless providers.[9]

III. RESILIENCE AND RAPID RESTORATION REQUIRE ENHANCED COORDINATION AND COLLABORATION.

Multiple stakeholders responding to a disaster event make important contributions to the recovery effort. For example, electric power companies work to restore power to cell sites, homes, enterprises, government facilities, and of course, the state and local emergency response officials responsible for coordinating these stakeholders on-the-ground. To enhance resiliency coordination and collaboration among communications and electric power companies, CTIA helped launch the Cross-Sector Resiliency Forum which facilitates contact information for

---

[8] *The Wireless Industry Responds to 2022 Hurricane Season*, CTIA Blog (Sept. 28, 2022), https://www.ctia.org/news/the-wireless-industry-responds-to-2022-hurricane-season.

[9] *See Resilient Networks Order* ¶ 33; *see also id*., Statement of Commissioner Geoffrey Starks ("The after-action reports we require today are also critically important. They'll help us develop the facts we need to monitor and learn from the Framework's implementation, and to improve our situational awareness during disasters.").

coordination before, during, and after an event, fosters cross-industry participation in exercises, workshops and summits, and develops targeted initiatives to promote overall resiliency.

CTIA and its member companies also have a long history of engaging in CISA's National Security and Emergency Preparedness efforts, including the National Coordinating Center for Communications ("NCCC"), a forum in which wireless operators participate in "blue skies" Emergency Support Function-2 exercises, share planning and network status information during an NSEP event, and coordinate response activities.

With wireless providers already engaged in the NCCC process, CISA's Incident Communications Activity Report should focus on information from state and local emergency response officials, with the goal of yielding lessons learned and best practices for public safety stakeholders, as well as new planning activities and exercises, to further advance resiliency during future disaster events.

IV. CISA'S INCIDENT COMMUNICATIONS ACTIVITY REPORT CAN BEST CONTRIBUTE TO ENHANCING RESILIENCY BY FOCUSING ON PUBLIC SAFETY SERVICES MANAGED OR CONTROLLED BY STATE AND LOCAL EMERGENCY RESPONSE OFFICIALS.

CISA's proposed definition of "public safety communications technologies" for public safety officials to report in the Incident Communications Activity Report includes "Cellular, Tactical Information Technology, Emergency Alert Systems, Land Mobile Radio, Satellite, 9-1-1 and emergency communications centers." To ensure that Incident Communications Activity Reports yield relevant and accurate information, CISA should ensure that the reports focus on "public safety communications technologies" controlled by reporting state or local emergency response officials.

State and local public safety officials have direct control and knowledge over certain public safety communications capabilities that they manage, such as Tactical Information

Technology, Land Mobile Radio, and Emergency Communications Centers. Information about the resilience of these services during a disaster event will be relevant to CISA, and reporting public safety officials will have direct knowledge to contribute.

While state or local public safety officials may contract for public safety-focused "cellular" services (e.g., Wireless Priority Services), the FCC already collects information about the availability of commercial communications services directly from providers during a disaster event through DIRS and shares that information with CISA. Through DIRS, wireless providers file reports that provide the FCC, emergency response officials, and the public with significant information about the availability of wireless services during disaster events. DIRS reports provide a daily snapshot of the status of network services, including the number of cell site outages, the cause of such outages (i.e., due to damage, loss of transport, or loss of power), and the number of cell sites operating on backup power. While cell site outage reporting does not account for overlapping cell site coverage that increasingly maintains coverage even where an isolated site is down, overall DIRS reports provide critical information regarding each disaster event, including efforts to overcome power or transport issues to restore service to impacted areas.[10]

The FCC shares DIRS information with federal and state emergency response partners, including CISA, as well as the public. As CISA already has access to DIRS information collected by the FCC, CISA should refrain from directing state and local public safety officials from opining on the general availability of commercial "cellular" services during a disaster event through Incident Communications Activity Reports.

---

[10] *See, e.g.*, *The Public Safety and Homeland Security Bureau Announces the Activation of the Disaster Information Reporting System for Communications Impacted by Hurricane Ian in Florida*, Public Notice, DA 22-1014 (rel. Sept. 27, 2022).

Further, CISA should ensure that information about Emergency Alert Systems and 9-1-1 services provided through Incident Communications Activity Reports is focused on the parts of those systems directly controlled or managed by state or local public safety officials. For example, it may be useful to understand the impacts of a disaster event on the technologies that state or local public safety officials use to originate a Wireless Emergency Alert ("WEA") to the Federal Emergency Management Agency's Integrated Public Alert & Warning System's gateway. This aspect of WEA—focused on state or local public safety officials' efforts to originate a WEA message—is distinct from the distribution of that message, which is the responsibility of participating commercial mobile service providers. The FCC is already considering how to evaluate the performance of WEA, including the distribution and receipt of WEA messages.[11]

The same holds true for 9-1-1 services. It may be useful for CISA to understand the impacts of a disaster event on the technologies and services used by public safety answering points ("PSAP") and emergency communications centers to respond to 9-1-1 communications, including the Emergency Services IP Transport Network, Access and NG9-1-1 Core Services, and PSAP Terminating Equipment/Call-taking Support subsystems (i.e., Computer Aided Dispatch, Management Information Systems, Dispatching Equipment, etc.).[12] Those capabilities of emergency communications centers are distinct from the availability of commercial communications services used to originate 9-1-1 communications. Notably, the FCC recently

[11] *See Wireless Emergency Alerts; Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, Further Notice of Proposed Rulemaking, FCC 22-31 (rel. Apr. 21, 2022).

[12] *See Task Force on Optimal PSAP Architecture – Adopted Final Report*, FCC, at 21 (Jan. 29, 2016), https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf.

adopted new rules to ensure that local emergency communications centers are aware of the status of commercial communications services that can originate 9-1-1 communications.[13]

Focusing Incident Communications Activity Reports on "public safety communications technologies" controlled by state and local officials would yield new insights into emergency response and avoid duplicating the FCC's disaster-event information collection. CISA can also ensure that Incident Communications Activity Reports collect information about "public safety communications technologies" from sources with direct knowledge and do not conflict with information provided to the FCC. And importantly, CISA has access to DIRS information the FCC collects directly from communications service providers during and after disaster events.

However, if information about commercial communications services is part of the information reported through Incident Communications Activity Reports, CISA should direct reporting state and local officials to coordinate with commercial providers to ensure that the reported information is accurate. For example, wireless providers use a variety of deployable assets, such as Cells On Wheels, Cells On Light Trucks, and portable generators, to maintain and restore services in areas impacted by a disaster event. Only commercial wireless providers would have complete knowledge about the deployment of those assets.

Finally, CISA should protect information collected about commercial communications services from public disclosure pursuant to Exemption 4 of the Freedom of Information Act.[14] Confidential treatment of this information is consistent with the practices of the FCC, which

---

[13] *See Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications; Improving 911 Reliability; New Part 4 of Commission's Rules Concerning Disruptions to Communications*, Second Report and Order, FCC 22-88 (rel. Nov. 18, 2022).

[14] *See* 5 U.S.C. § 552(b)(4); *Food Mktg. Inst. v. Argus Leader Media*, 139 S. Ct. 2356, 2365-66 (2019); 6 C.F.R. § 5.7.

treats information regarding commercial communications services submitted to the agency under Part 4 of its rules as presumptively confidential and not available for public inspection.[15]

V. CONCLUSION.

As described herein, the wireless industry shares the mission of CISA's Emergency Communications Division to promote communications used by emergency responders and government officials to keep America safe, secure, and resilient. In order to avoid duplicating the FCC's incident reporting efforts with commercial wireless providers, CISA should ensure that the Incident Communications Activity Reports are focused on "public safety communications technologies" controlled by reporting state or local emergency response officials. However, if information about commercial communications services is requested as part of the information reported through Incident Communications Activity Reports, CISA should direct reporting state and local officials to coordinate with commercial providers to ensure that the reported information is accurate. CISA should also treat information about commercial communications services as confidential.

Respectfully submitted,

Michael Mullinix

Michael Mullinix
Assistant Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Amy Bender
Vice President, Regulatory Affairs

[15] *See* 47 C.F.R. § 4.2.

CTIA
1400 16th Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

Dated: December 19, 2022