FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 4

[PS Docket No. 15–80; FCC 21–34; FRS 20221]

Disruptions to Communications

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) adopts final rules to provide direct, read-only access to Network Outage Reporting System (NORS) and Disaster Outage Reporting System (DIRS) filings to agencies of the 50 states, the District of Columbia, tribal nations, territories, and Federal Government that have official duties that make them directly responsible for emergency management and first responder support functions, including by: Allowing these agencies to share NORS and DIRS information with agency officials, first responders, and other individuals with a ''need to know'' who cannot directly access NORS and DIRS and yet play a vital role in preparing for, or responding to, events that threaten public safety; allowing participating agencies to publicly disclose aggregated and anonymized information derived from NORS or DIRS filings; conditioning a participating agency's direct access to NORS and DIRS filings on their agreement and ability to preserve the confidentiality of the filings and not disclose them absent a finding by the Commission allowing the disclosure; and establishing an application process that would grant eligible agencies access to NORS and DIRS after those agencies certify to certain requirements related to maintaining the confidentiality of the data and the security of the databases.

DATES: This rule is effective September 30, 2022.

FOR FURTHER INFORMATION CONTACT: For further information, contact Saswat Misra, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418–0944 or via email at *Saswat.Misra@fcc.gov.*

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Second Report and Order, FCC 21–34, adopted on March 17, 2021 and released on March 18, 2021. The document is available for download at *https://docs.fcc.gov/public/attachments/FCC-21-34A1.pdf.* To request this document in accessible formats for people with disabilities (*e.g.,* Braille, large print, electronic files, audio format, etc.) or to request reasonable accommodations (*e.g.,* accessible format documents, sign language interpreters, CART, etc.), send an email to *fcc504@fcc.gov* or call the FCC's Consumer and Governmental Affairs Bureau at (202) 418–0530 (voice), (202) 418–0432 (TTY).

The Federal Communications Commission may delay this effective date by publishing a document in the **Federal Register**.

Paperwork Reduction Act:

The Second Report and Order requires service providers to make adjustments to their NORS reporting processes to accommodate the Commission's adjustments to its NORS web-based form pursuant to section 47 CFR 4.11. These adjustments and the new requirement that agencies file certification forms, pursuant to 47 CFR 4.2, to request access to NORS and DIRS reports, constitute a modified information collection. The information collection requirements contained in the rules that require OMB approval are subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104–13. The information collection will be submitted to OMB for review under 47 U.S.C. 3507(d), and will not take effect until it is approved by OMB.

Congressional Review Act:

The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this Order to Congress and the Government Accountability Office, pursuant to 5 U.S.C. 801(a)(1)(A).

Synopsis:

I. Introduction

1. Section 1 of the Communications Act of 1934, as amended (the Act), charges the Commission with ''promoting safety of life and property through the use of wire and radio communications.'' 47 U.S.C. 151. This statutory objective and statutory authorities cited below have supported the Commission's institution of outage reporting requirements, codified in part 4 of our rules, that require providers to report network outages that exceed specified magnitude and duration thresholds. The outage data that the Commission collects pursuant to part 4 provide critical situational awareness that enables the Commission to be an effective participant in emergency response and service restoration efforts, particularly in the early stages of communications disruption.

2. Currently, the Commission collects network outage information in the NORS and infrastructure status information in the DIRS. This information is sensitive for reasons concerning national security and commercial competitiveness, and the Commission thus treats it as presumptively confidential. The Commission makes this information available to the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center but does not share the information more broadly with other Federal, state, or local partners. However, in a 2016 Report and Order and Further Notice, the Commission found that state and Federal agencies would benefit from direct access to NORS data and that ''such a process would serve the public interest if implemented with appropriate and sufficient safeguards.'' 81 FR 45055, 45064 (July 12, 2016) (*2016 Report and Order and Further Notice*).

3. Today's Order bridges this gap and promotes better information sharing and awareness during times of emergency. It creates a framework to provide state, Federal, local, and Tribal partners with access to the critical NORS and DIRS information they need to ensure the public's safety while preserving the presumptive confidentiality of the information. Today's actions will ensure that these public safety officials can appropriately and effectively leverage the same reliable and timely network outage and infrastructure status information as the Commission when responding to emergencies.

II. Background

4. *Network Outage Reporting System or NORS.* In 2004, the Commission adopted rules that require outage reporting for communications providers, including wireline, wireless, paging, cable, satellite, VoIP, and Signaling System 7 service providers, to address ''the critical need for rapid, complete, and accurate information on service disruptions that could affect homeland security, public health or safety, and the economic well-being of our Nation, especially in view of the increasing importance of non-wireline communications in the Nation's communications networks and critical infrastructure.'' These rules currently do not extend to broadband networks. In 2016, the Commission sought comment on whether its part 4 rules should be updated to implement a proposed system for the mandatory reporting of broadband network outages and other disruptions, including those based on performance degradation. The proposals

in the *2016 Report and Order and Further Notice* remain pending.

5. Under these rules, certain service providers must submit outage reports to NORS for outages that exceed specified duration and magnitude thresholds. Service providers are required to submit a notification to NORS generally within two hours of determining that an outage is reportable to provide the Commission with timely preliminary information. The service provider must then either (i) provide an initial report within three calendar days, followed by a final report with complete information on the outage within 30 calendar days of the notification; or (ii) withdraw the notification and initial reports if further investigation indicates that the outage did not in fact meet the applicable reporting thresholds.

6. All three types of NORS filings—notifications, initial reports, and final reports—contain service disruption or outage information that, among other things, include: The reason the event is reportable, incident date/time and location details, state affected, number of potentially affected customers, and whether enhanced 911 (E911) was affected. The Commission analyzes NORS outage reports, in the short-term, to assess the magnitude of major outages and, in the long-term, to identify network reliability trends and determine whether the outages likely could have been prevented or mitigated had the service providers followed certain network reliability best practices. Information collected in NORS has contributed to several of the Commission's outage investigations and recommendations for improving network reliability.

7. NORS filings are presumed confidential and thus are withheld from routine public inspection. 47 CFR 0.457(d)(vi), 4.2; 80 FR 34321 (June 16, 2015) (*2015 Notice*). The Commission grants read-only access to outage report filings in NORS to the National Cybersecurity and Communications Integration Center at DHS, but does not directly grant access to other Federal agencies, state governments, or other entities. DHS, however, may share relevant information with other Federal agencies at its discretion. The Commission also publicly shares limited analyses of aggregated and anonymized data to address collaboratively industry-wide network reliability issues and improvements.

8. *Disaster Information Reporting System or DIRS.* In the wake of Hurricane Katrina, the Commission established DIRS as a means for service providers, including wireless, wireline cable service providers, and broadcasters, to voluntarily report to the Commission their communications infrastructure status and situational awareness information during times of crises. The Commission recently required a subset of service providers that receive Stage 2 funding from the Uniendo a Puerto Rico Fund or the Connect USVI Fund to report in DIRS when it is activated in the respective territories. DIRS, like NORS, is a web-based filing system. The Commission analyzes infrastructure status information submitted in DIRS to provide public reports on communications status during DIRS activation periods, as well as to help inform investigations about the reliability of post-disaster communications.

9. DIRS filings are also presumed confidential and disclosure of information derived from those filings is limited. The Commission grants direct access to the DIRS database to the National Cybersecurity and Communications Integration Center at DHS. The Commission also prepares and provides aggregated DIRS information, without company identifying information, to the National Cybersecurity and Communications Integration Center, which then distributes the information to a DHS-led group of Federal agencies tasked with coordinating disaster response efforts, including other units in DHS, during incidents. Agencies use the analyses for their situational awareness and for determining restoration priorities for communications infrastructure in affected areas. The Commission also provides aggregated data, without company-identifying information, to the public during disasters.

10. *Expanding Access to NORS and DIRS.* In a *2015 Notice,* the Commission proposed to grant state governments ''read-only access to those portions of the NORS database that pertain to communications outages in their respective states.'' The Commission also asked if this access should extend beyond states and include ''the District of Columbia, U.S. territories and possessions, and Tribal nations.'' The Commission proposed to condition access on a state or other agency's certification that it ''will keep the data confidential and that it has in place confidentiality protections at least equivalent to those set forth in the Federal Freedom of Information Act (FOIA).'' The Commission sought comment on other key implementation details, including how to ''ensure that the data is shared with officials most in need of the information while maintaining confidentiality and assurances that the information will be properly safeguarded.'' Similarly, the Commission sought comment on sharing NORS filings with Federal agencies besides the Department of Homeland Security pursuant to certain safeguards to protect presumptively confidential information.

11. In a *2016 Report and Order and Further Notice,* the Commission found that the record reflected broad agreement that these agencies would benefit from direct access to NORS data and that ''such a process would serve the public interest if implemented with appropriate and sufficient safeguards.'' The Commission determined that providing agencies with direct access to NORS filings would have public benefits but concluded that the process required more development for ''a careful consideration of the details that may determine the long-term success and effectiveness of the NORS program.''

12. Finding that the record was not fully developed and that the ''information sharing proposals raise[d] a number of complex issues that warrant[ed] further consideration,'' the Commission directed the Public Safety and Homeland Security Bureau (PSHSB) to further study and develop proposals regarding how NORS filings could be shared with agencies in real time, keeping in mind the information sharing privileges already granted to DHS. The Bureau subsequently conducted *ex parte* meetings to solicit additional viewpoints from industry, state public service commissions, trade associations, and other public safety stakeholders on the issue of granting state and Federal Government agencies direct access to NORS and DIRS filings.

13. In a February 2020 Second Further Notice, the Commission proposed to: (i) Grant direct, read-only access to the Commission's NORS and DIRS filings to agencies acting on behalf of the Federal Government, the 50 states, the District of Columbia, Tribal Nations, and the U.S. territories that demonstrate that they reasonably require access to prepare for, or respond to, an event that threatens public safety pursuant to their official duties (*i.e.,* that have a ''need to know''); (ii) authorize participating agencies to share copies of these filings, and any other confidential information derived from the filings, within or outside their agencies when a recipient also has a ''need to know,'' subject to certain safeguards, (iii) allow the recipient to further share the confidential NORS and DIRS information, directly or in summarized form, with additional recipients; and (iv) authorize any recipient to freely

share aggregated and anonymized information derived from the NORS and DIRS filings of at least four service providers. 85 FR 17818 (Mar. 31, 2020) (*Second Further Notice*).

14. The Commission proposed to safeguard the confidentiality of NORS and DIRS information by conditioning an agency's direct access on agreements to: (i) Treat NORS and DIRS filings as confidential and not disclose them, absent a finding by the Commission allowing the disclosure; and (ii) provide timely notification to the Commission when the agency receives a request from a third party to release NORS or DIRS filings or related records and when changes to statutes or rules would affect the agency's ability to adhere to the Commission's required confidentiality protections.

III. Second Report and Order

15. With this Order, we conclude that directly sharing NORS data with state and Federal agencies, subject to appropriate and sufficient safeguards, is in the public interest, and we extend this finding to include the sharing of DIRS data. We limit eligibility for direct access to our NORS and DIRS databases to ''need to know'' agencies acting on behalf of the Federal Government, the 50 states, the District of Columbia, Tribal Nations, and the U.S. territories. We also decide which agency responsibilities constitute a ''need to know'' and limit a participating agency's use of this information to those purposes. We allow these agencies to share confidential information derived from NORS and DIRS filings with non-credentialed individuals at the participating agency and at non-participating agencies on a strict ''need to know'' basis. We also allow recipients to release aggregated and anonymized NORS and DIRS information to the public and offer guidance on how that aggregation and anonymization should be performed.

16. To preserve the sensitive nature of NORS and DIRS filings, we adopt various safeguards, including limiting agency access to events occurring within an agency's jurisdiction; limiting access to five user accounts; requiring initial and annual security training; and requiring agencies to certify that they will take appropriate steps to safeguard the information contained in the filings, including notifying the Commission of unauthorized or improper disclosure. We require that participating agencies certify they will treat the information as confidential and not disclose the information absent a finding by the Commission that allows them to do so. We decline to allow non-participating agencies to further share the information with others. Under today's Order, we hold participating agencies responsible for any inappropriate disclosures of information by the non-participating agencies with which they share information, including by retaining the ability to terminate participating agencies' direct access to NORS and DIRS.

A. Sharing NORS Filings With State, Federal and Other Agencies

17. In the *Second Further Notice,* the Commission tentatively concluded ''that sharing NORS data with state and Federal agencies would serve the public interest—provided that appropriate and sufficient safeguards were implemented'' and sought to refresh the record to inform next steps. We now observe that industry, public safety organizations, and government agency commenters overwhelmingly support the Commission's proposal. We agree with commenters concluding that sharing NORS filings with other agencies will improve situational awareness during and after disasters, enable agencies to better assess the public's ability to access emergency communications, and assist with the coordination of emergency response efforts.

18. The Alliance for Telecommunications Industry Solutions (ATIS), however, maintains that while it ''supports efforts that aid in restoral of communications services and that help save lives,'' the sharing of NORS reports will ''generally not serve such purposes'' and NORS reports contain information that is not relevant to public safety. ATIS also argues that specific NORS fields should not be shared with agencies.

19. We reject ATIS's view as it is controverted by a number of commenters explaining, with detailed examples and based on knowledge of their own day to day responsibilities and operations, why the information contained in NORS filings is relevant to public safety by assisting in rapid communications service restoration and enhancing situational awareness. For example, the Montrose Emergency Telephone Service Authority (METSA) believes that if the Colorado Public Utilities Commission (COPUC) had been granted NORS access following a July 2019 fiber cut, ''the COPUC could have assisted with generalized information regarding areas which were truly impacted by the outage.'' In another example, Massachusetts Department of Telecommunications and Cable (MDTC) believes that direct access to NORS data would have provided it, local official and town residents, businesses, and government offices with ''timely, and therefore, actionable'' information about a recent wireline telephone service outage. MDTC also believes that access would have helped providers avoid the burden of being contacted multiple times by multiple parties.

B. Sharing DIRS Filings With State, Federal and Other Agencies

20. In the *Second Further Notice,* the Commission also proposed sharing DIRS filings with eligible state and Federal agencies and sought comment on the anticipated benefits of sharing DIRS filings. We adopt this proposal, finding that sharing DIRS filings will enhance public safety by improving participating agencies' situational awareness regarding infrastructure status and helping to inform their decisions on how to allocate resources. No commenters oppose the Commission's DIRS proposal. Rather, many agree that sharing DIRS filings will provide the benefits cited by the Commission in the *Second Further Notice,* including improving the effectiveness of response and recovery efforts during and after disasters and providing stakeholders with actionable status of communications outages. Communications Workers of America (CWA) states that ''information contained in the DIRS will be very helpful to understand the status of communications infrastructure in the impacted area and to set restoration priorities'' following major events such as wildfires and flooding. Other commenters underscore that access to both DIRS and NORS are vital to aid in situational awareness and emergency response initiatives because in the counties where DIRS has been activated, NORS reporting obligations are typically suspended for the duration of the DIRS activation.

21. Some commenters urge the Commission to make DIRS reporting mandatory. We decline to do so, as this issue is outside of the scope of this rulemaking. We agree with T-Mobile that such action would go ''beyond the question of sharing NORS and DIRS data and the manner in which the information should be shared.'' We also note that as our priority with this proceeding is ensuring that agencies begin to receive critical information about service outages to assist them in their service restoration initiatives, technical changes that may be necessitated by making DIRS reporting mandatory could delay such access.

C. Scope of Direct Access

22. *Eligibility for direct access.* In the *Second Further Notice,* the Commission proposed that direct access to NORS and DIRS be limited to agencies acting on behalf of the Federal Government, the 50 states, the District of Columbia, Tribal Nations, and the U.S. territories (including Puerto Rico and the U.S. Virgin Islands). We adopt this proposal.

23. The majority of commenters agree with this proposal, typically without significant comment. For example, T-Mobile remarks that limiting direct access in this way strikes an appropriate balance between disseminating NORS and DIRS information to those who most need it (*i.e.,* to save lives and property) and safeguarding the information's confidential nature. The California Public Utilities Commission believes that Tribal Nation eligibility is appropriate since Tribal Nation governments have oversight responsibility for public safety matters in their lands in the same manner as the other entities that the Commission has identified for direct access. We find that limiting direct access to NORS and DIRS filings is necessary to limit the risk for the over disclosure of sensitive and confidential information and to ensure administrative efficiency. While the Commission proposed to disallow direct access by local agencies, it proposed mechanisms to ensure that local agencies and related entities and individuals could indirectly access NORS and DIRS information on a case-by-case basis. We adopt some of these mechanisms today.

24. We reject Colorado Public Utilities Commission's view that Tribal Nation entities should be eligible for direct access only if they do not participate directly in a state 911 program or have their own 911 program. We find no reason to treat Tribal Nations differently than state agencies with respect to NORS or DIRS information sharing, and commenters have offered no new evidence to warrant such a departure. The Colorado Public Utilities Commission's approach appears to assume that NORS and DIRS information is only beneficial as it relates to improving 911 service. In contrast, we find that jurisdictions, including Tribal lands, can benefit from NORS and DIRS information for uses beyond improved 911 performance. This is corroborated, for example, by The Utility Reform Network's comments evidencing that agencies serving Tribal lands would have been better able to transmit emergency evacuation alerts during the 2019 California wildfire event had they had access to outage information. We find that Tribal Nations have a need for NORS and DIRS information regardless of their participation in a state's 911 program.

25. We reject the position of some commenters that at the state or local level, only state-based fusion centers (*i.e.,* state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information among state, local, Tribal, territorial, Federal and private sector partners) should be eligible to directly access NORS and DIRS data. These commenters argue that fusion centers are uniquely qualified for direct access because they work closely with state public safety agencies, are familiar with handling, analyzing, and summarizing sensitive information, and typically operate around the clock or because of their ''connection to the Federal Government.'' We are not persuaded.

26. Our experience over many years indicates that many other types of agencies have experience in coordinating with public safety agencies, handling sensitive information, and working tirelessly when disasters strike. No commenter has argued or provided evidence that fusion centers have specific expertise in interpreting NORS and DIRS outage information such that they alone should disseminate it. Fusion centers are not uniquely or solely qualified in this regard. We therefore find no reason to preclude otherwise eligible state agencies from accessing NORS and DIRS information, especially if such access would enhance public safety response and situation awareness. Contrary to views posited by the IACP, we find no administrative benefit in limiting accessibility to NORS and DIRS information to fusion centers. Instead, by exercising our administrative oversight for reviewing each application for access to NORS and DIRS, as detailed in today's Order, the Commission will be better able to ensure that NORS and DIRS information is used appropriately.

27. *Local Agencies.* We are not persuaded by commenters who argue that local agencies should be eligible for direct access to NORS and DIRS because they have the primary responsibility for responding to emergencies. We find the potential benefits of doing so are outweighed by the substantial risks and burdens of providing local agencies with direct access.

28. As noted by some commenters, local entity governments typically do not have the level of experience navigating the kinds of outage and infrastructure status information contained in NORS and DIRS filings that state agencies do. We agree with USTelecom that providing direct access to local entities would likely exponentially increase the number of participating entities, thus complicating administration and increasing opportunities for erroneous disclosure of confidential information. We believe such a large increase would render it difficult or impossible for the Commission to effectively administer the sharing framework. Instead, we believe that providing local entities indirect access, through participating agencies with direct access, will sufficiently support the public safety needs of localities while striking a fair balance between sharing NORS and DIRS information and minimizing the potential for unauthorized disclosure.

29. We similarly reject the views of some commenters that request that the Commission provide local entities with direct access purportedly so that state agencies are not burdened by, and delays are not created in, requiring them to provide this information to local entities themselves. Today's framework does not require, but only allows, these agencies to share NORS and DIRS information with local entities. As the National Association of Regulatory Utility Commissioners (NARUC) points out, agencies collectively have more resources dispersed across the country than the Commission. We find that the responsibility of disseminating information to local entities is most efficiently placed on this range of state and other agencies, each with specific knowledge and incentives to further public safety in its own jurisdiction.

30. We also are not convinced that allowing an agency with direct access to share its credentials with an associated local entity would alleviate our administrative burdens and disclosure risk concerns, as opined by the Texas 9–1–1 Entities. We reject this approach because it would allow direct access to NORS and DIRS by local agencies whose certifications have not been reviewed and approved by the Commission and are not directly accountable to the Commission. We find that a credential sharing scheme would unacceptably increase the risk that our training and other procedural safeguards would not be implemented, which would make it more likely that NORS and DIRS filings could be improperly used or disclosed.

31. We also find unconvincing, the view of one commenter that ''advocates, researchers and the public,'' among others, should be eligible for direct access purportedly ''to hold

telecommunications providers accountable and monitor the communications rights of impacted communities.'' This approach fails to address the Commission's findings that have long treated NORS and DIRS filings as presumptively confidential to further national security and protect commercially sensitive information. We find that granting such broad access to NORS and DIRS information would effectively render that treatment moot and thereby detract from these objectives.

32. *Eligible agencies must have a ''need to know.''* In the *Second Further Notice,* the Commission proposed that direct access to NORS and DIRS be limited to eligible agencies that have a ''need to know,'' which was defined as ''reasonably requir[ing] access to the information in order to prepare for, or respond to, an event that threatens public safety, pursuant to its official duties.'' We today adopt a modified definition of ''need to know'' that includes only agencies that have official duties that make them directly responsible for emergency management and first responder support functions.

33. Most commenters agree that direct access should be limited to agencies with a ''need to know'' to prevent the over-disclosure of sensitive NORS and DIRS information, though commenters differ in their views on the appropriate definition of the term. We are persuaded by Verizon that a ''need to know'' should be defined to refer to an agency ''having official duties making it directly responsible for emergency management and first responder support functions.'' We find that this definition best achieves the goal of ensuring that only agencies with the greatest and most relevant public safety needs have access to the sensitive information contained in our NORS and DIRS databases. We note that this definition for ''need to know'' is more specific and narrow than what the Commission proposed in the *Second Further Notice* and will minimize the number of disputes over which agencies qualify for access, thus preserving public safety resources. We confirm NCTA's view that an ''event'' giving rise to a ''need to know'' may be either natural or ''manmade.'' While we do not exhaustively enumerate here every type of agency that may qualify for access under our adopted ''need to know'' standard, we expect that qualifying agencies will include state homeland security and emergency management departments, state first responder departments (including fire and law enforcement departments), and state public utility (or public service) commissions. We agree with New York State Public Service Commission and the Public Service Commission of the District of Columbia that state public utility and service commissions typically support public safety and emergency response efforts, including by coordinating the restoration of telecommunications in their jurisdictions.

34. In view of the record, we disagree with the views of the Competitive Carriers Association and T-Mobile who argued that the Commission's earlier proposed definition of ''need to know'' struck an appropriate balance between ensuring that an appropriate set of agencies will have access to NORS and DIRS data for their public safety efforts and reducing the likelihood of improper disclosure. For the reasons noted above, we find that a more objective and narrower standard is necessary for today's program to be administrable and to ensure that the sensitive information in NORS and DIRS filings is not disseminated broadly beyond a small set of core agencies in each state or other jurisdiction.

35. *Demonstrating a ''need to know.''* An agency applying for direct access to NORS and DIRS must demonstrate its ''need to know'' by citing to statutes or other regulatory authority that establishes it has official duties making it directly responsible for emergency management and first responder support functions.

36. We agree with Verizon and NCTA that an objective showing of legal authority, in the form of statues or other regulatory bases, is necessary as part of the application process to ensure that only qualified agencies have direct access to NORS and DIRS filings. We find that the approach we adopt today will avoid protracted disputes and subjective interpretations about what roles and responsibilities an agency may have during an emergency and will guard against the over-disclosure of sensitive NORS and DIRS information.

37. *Scope of Use.* In the *Second Further Notice,* the Commission proposed that NORS and DIRS information accessed by participating agencies be used only for public safety purposes. We adopt this proposal and clarify that the only valid public safety purposes are the same purposes that would give rise to a ''need to know,'' *i.e.,* carrying out emergency management and first responder support functions that an agency is directly responsible for pursuant to its official duties.

38. Several commenters seek confirmation that certain use cases are permitted. We confirm commenters' views that a participating agency's dissemination of information to other individuals responsible for preparing and responding to disasters is an acceptable use. We also confirm commenters' views that the assessment of emergency notification options available in areas impacted by an outage or disaster, including determining whether Wireless Emergency Alert messages can be delivered and, if not, coordinating alternate methods of notification, is an acceptable use. We further confirm the views of the Telecommunications Regulatory Bureau of Puerto Rico and other commenters that identifying trends and performing analyses designed to make long-term improvements in public safety outcomes are acceptable uses. We agree that these long-term efforts are critical for preparing for events that threaten public safety in ways that will reduce the loss of life and property in future outage and disaster scenarios. We are similarly persuaded by the Massachusetts Department of Telecommunications and Cable, which explains the potential value of NORS and DIRS information in its analyses used to improve service and avoid future outages, and the Michigan Public Service Commission, which explains that the information would assist in understanding the nature of outages, ultimately resulting in more resilient networks. We find that these uses reflect carrying out emergency management and first responder support functions by informing the public of danger, or preparing in advance for such danger, to avoid the loss of life and property.

39. We expressly forbid the use of NORS and DIRS information obtained through the procedures we adopt today for non-emergency-related regulatory purposes, including merger review, consumer protection activities, contract disputes with a state, or the release of competitive information to the public. We agree with commenters that such uses of NORS and DIRS data would be inconsistent with the public safety purposes for which the sharing framework was created. Moreover, such uses could create counter-productive incentives for providers to supply superfluous information in their NORS and DIRS disclosures thereby diminishing the public safety value of these filings.

40. *911 fee diversion.* In the *Second Further Notice,* the Commission sought comment on whether it should exclude from eligibility agencies located in states that have diverted or transferred 911 fees for purposes other than 911 and how it should address agency access in states that have inadequately responded to Commission inquiries about their

practices for using 911 fees. We decline to exclude agencies located in fee diverting states from eligibility in today's information sharing framework.

41. Nearly all commenters reject the exclusion of agencies on grounds that they are located in states that have engaged in fee diversion or provided an inadequate disclosure of their fee practices to the Commission. We agree with those commenters who remark that access to NORS and DIRS information, and the important public safety benefits associated therewith, should not be conditioned on whether a state engages in 911 fee diversion. We find this point particularly compelling since, as noted by Colorado Public Utilities Commission and NASNA, diversion may be an act of the state legislature rather than the agency seeking access to NORS and DIRS information.

42. We find that the benefits of providing NORS and DIRS information to entities in these states outweigh the possibility that withholding this information may incentivize legislatures to reconsider fee diversion decisions, particularly as no commenters offered evidence supporting this view. On September 30, 2020, the Commission adopted a Notice of Inquiry seeking comment on ways to dissuade states and territories from diverting fees collected for 911 to other purposes, and on the effects of 911 fee diversion. We are not persuaded otherwise by T-Mobile's conclusory statement supporting the exclusion of agencies, which in relying on comments filed in an unrelated proceeding, fails to address the potential negative impacts of withholding NORS and DIRS information from agencies or the extent to which doing so would motivate legislatures to reconsider their fee diversion decisions.

D. Confidentiality Protections

43. *Direct access conditioned on confidential treatment by agencies.* In the *Second Further Notice,* the Commission proposed that the Commission make all confidentiality determinations implicating the release of confidential NORS and DIRS information pursuant to today's program. The Commission proposed that a participating agency only receive direct access to NORS and DIRS filings if it could agree, under its governing laws, that when it received a request to release NORS or DIRS information under open record laws in its jurisdiction, it would defer to and comply with a Commission determination and not disclose the filings other than as expressly allowed in today's Order or any subsequent Commission determinations. We adopt this proposal.

44. The majority of commenters, including state and local entities, and industry advocacy organizations, support this approach. We agree with Verizon that this approach is ''essential'' to protecting NORS and DIRS information, because requests for disclosure of confidential information would be determined uniformly rather than being left to a patchwork of varying open records law standards among jurisdictions. We also agree with the IACP, which stresses that without the Commission's role in reviewing requests, public safety entities could face ''nuisance lawsuits'' and have their scarce public safety resources diverted as they become ''embroiled in legal challenges or extended discussions regarding the confidentiality of NORS and DIRS information.'' We find that our approach would create a necessary, simple mechanism to control the flow of confidential NORS and DIRS information, even when state and other open records laws vary.

45. Commenters confirm that this proposal is workable in practice. A number of state public utility commissions identify exemptions in their open records laws that allow them to defer to the Commission's FOIA determination in place of making their own. Moreover, no commenter contends that there is a jurisdiction that would not be able to defer to the Commission pursuant to the jurisdiction's open records and other relevant laws. We agree with The Utility Reform Network that state, Federal and Tribal Nation entities are well versed in handling confidential material based on their other programs and that they would therefore be able to adhere to today's confidentiality requirements. We similarly agree with the California Public Utilities Commission and Massachusetts Department of Telecommunications and Cable, which bolster this point by noting that today's confidentiality requirements are familiar to many participating agencies because they resemble ones the Commission separately established for the sharing of presumptively confidential data with states in separate programs involving the Form 477 database and the North American Numbering Plan Administrator database.

46. We are unpersuaded on the current record that the presumption of confidentiality for all NORS and DIRS information is not fully warranted, as some commenters argue. While these commenters contend that NORS and DIRS information often does not contain information that is sensitive for national security reasons, no commenter provides practical guidance on how to distinguish at an operational level those reports that contain such sensitive national security information (or sensitive business information) from those that do not. Because we did not seek comment on this question, and because the record is incomplete as to the types of information, or the specific fields in NORS and DIRS, that these commenters believe should not receive confidential treatment, we are not in a position today to decide upon the merits of these views. We also find that these commenters fail to address the possibility that a collection of NORS and DIRS filings could reflect patterns that implicate national security, even when filings taken individually may not. Moreover, given that we maintain the presumption of confidentiality as to our own use of NORS and DIRS data, we find it logical to require that participating agencies, and those who receive information from them, be held to the same type of confidentiality standards. To do otherwise would allow these entities to disclose the data in ways that would contradict and render meaningless the Commission's own presumptively confidential treatment. Based on the lack of new information provided by commenters on the current record, we decline to reverse at this time the Commission's long-held view that NORS and DIRS information warrants confidential treatment. The Commission acknowledges that some commenters assert that public access to some outage information would benefit the public, and nothing we do today permanently forecloses us from examining this issue further in the future.

47. We also find unpersuasive the view of the California Public Utilities Commission that ''industry's perception'' of the confidentiality of NORS and DIRS data is changing, merely because Verizon and other service providers have decided to increase their public disclosure of outage information around major communications outage events. On the contrary, we believe that a rollback of the Commission's presumption of confidentiality of NORS and DIRS data would actually have the opposite effect of discouraging companies from voluntarily taking meaningful incremental steps to make more information available.

48. We also reject NTCA's position that today's framework should go further and shield NORS and DIRS filings from any disclosure in response to a request filed under state-level FOIA-type laws. The approach we adopt today permits disclosure only when the

state defers to the Commission and the Commission makes a determination, based on the Federal FOIA standard, permitting the disclosure. Because the Commission will consider requests made under state-level open records laws identically to requests made under FOIA, NORS and DIRS information would not be better protected from inappropriate disclosure by specifically blocking from consideration any requests received by participating agencies under their open records laws. We also reject NARUC's view that the Commission's proposal is unnecessary since ''to avoid concerns [in] the tiny minority of States that have arguably deficient FOIA-type protections in-place,'' the Commission need only condition access to the data on states providing some level of confidential treatment. We have not found any practical way to identify the purported ''tiny minority'' of states that have deficient open records laws. Even among states that have ''non-deficient laws,'' we expect that the substance of those laws is likely to vary in ways that would result in the different treatment of certain NORS and DIRS data fields from jurisdiction to jurisdiction. In contrast, the Commission's proposal would advantageously provide a uniform confidentiality standard and thus better protect confidential NORS and DIRS information from unauthorized disclosure.

49. *Agency notifications to the Commission proposed in the Second Further Notice.* In the *Second Further Notice,* the Commission proposed to require that a participating agency notify the Commission: (i) Within 14 calendar days from the date the agency receives a request from third parties to disclose NORS filings and DIRS filings, or related records, pursuant to its jurisdiction's open record laws or other legal authority that could compel it to do so, and (ii) at least 30 calendar days prior to the effective date of any change in relevant statutes or rules (*e.g.,* its open records laws) that would affect the agency's ability to adhere to the confidentiality protections in this information sharing framework. We adopt these proposals.

50. Commenters generally support these proposals and no commenter expressly opposes them. We find that the 14-day notification we adopt today will allow the Commission take appropriate action, including (at the Commission's option) notifying an affected service provider so that the provider can supply its comments on the matter if permitted under the jurisdiction's open records law. We find that the 30-day notification we adopt today will provide the Commission with an opportunity to determine whether to terminate an agency's access to NORS or DIRS filings or take other appropriate steps as necessary to protect this information. As noted in the *Second Further Notice,* we find that these proposals will help ensure consistency in disclosure by many disparate agencies that will receive this information under the terms of today's Order and will instill confidence that submitted information will continue to be protected as it is today.

51. *Additional notifications proposed by commenters.* We reject the views of commenters that additional notifications from the Commission or participating agencies are necessary to ensure that service providers can dispute various types of requests for NORS and DIRS information and thus protect the confidentiality of their shared information. ATIS argues that we should require a notification from a participating agency within 14 days of when it receives a request to share NORS and DIRS data with a local agency. ATIS also argues that for both this notification and the 14-day disclosure request notification the Commission proposed in the *Second Further Notice,* the Commission should be required (as opposed to have the option) to notify service providers to allow them sufficient opportunity to provide any input. ATIS further argues that we should also require participating agencies to notify service providers at least 30 calendar days prior to the effective date of any change in relevant statutes or rules that could implicate the providers' filings. CenturyLink similarly argues that service providers should be made aware when a local agency receives access to NORS and DIRS data. ACA Connect contends that an agency should be required to submit, apparently to the Commission, the name of all recipients that it shares information with.

52. We reject these views, including to the extent they would require that participating agencies provide notification directly to service providers. Our rules require that the Commission provide notice to service providers, and allow them an opportunity for comment, when it receives FOIA requests for their NORS and DIRS filings. 47 CFR 0.461(d)(3). Today's rules require that a participating agency provide the Commission, not service providers, with notice when it receives a request for the NORS and DIRS filings under its state or other open-records laws. We find that the burden of requiring participating agencies to provide a voluminous number of new notifications to service providers on receipt of sharing requests (which are likely to be received when major outages or other public safety events are on-going) to be an unwarranted diversion of scarce public safety resources from state, Tribal Nation, and local agencies when they may be needed most. We further note that providers have the ability and incentive to monitor potential changes in confidentiality laws (where the providers operate) as a matter of general business practice, and we find it redundant and inefficient to ask participating agencies to commit their limited resources to this task. To address the concerns of record that providers would not receive notice when the Commission is notified of a request under state-level open records laws, Commission Staff will post a notification to the Commission's Electronic Filing Comment System (EFCS) in the present docket, on receipt of such notification from a participating agency, identifying the existence of the open records request, the jurisdiction under which the request was received and the service provider(s) whose filings are implicated by the request. Interested parties, including service providers, may use the push notification feature in ECFS to receive an alert when filings have been posted in the present docket, further facilitating prompt notification. We find that this approach appropriately balances providing notification to service providers of the existence of such requests with our concerns that requiring participating agencies to provide direct notifications to providers could be overly burdensome of scarce public safety resources.

53. We recognize, however, based on these comments, a need for increased accountability in how participating and non-participating agencies use NORS and DIRS information. We therefore adopt the requirement that each participating agency make available for Commission inspection, upon Commission request, a list of all localities for which the agency has disclosed NORS and DIRS data. The Commission may, at its discretion, share such lists with the implicated providers. While this requirement falls short of some commenters' requests for additional notifications, we find that it appropriately balances maintaining accountability on the part of participating agencies with minimizing the day-to-day burden on agencies for participating in the sharing program.

54. The Commission is aware that agencies that voluntarily elect to participate in this information sharing

framework may incur some costs due to the obligation to notify the Commission when they receive requests for NORS filings, DIRS filings, or related records and when there is a change in relevant statutes or laws that would affect the agency's ability to adhere to confidentiality protections. These costs include modest initial costs to review and revise their confidentiality protections in accordance with the framework we adopt in today's Order, and minimal reoccurring costs to notify the Commission as described above. We cannot quantify agency costs for these activities, which would vary based on each participating agency's particular circumstances, including the number of requests or changes in law that would necessitate notifications, as we lack the record evidence to quantify such benefits. This lack of quantification, however, does not diminish in any way the advantages of providing access to NORS and DIRS information to improve the safety of residents during times of telecommunications outage infrastructure distress. We conclude that the benefits of participation would likely exceed the costs for any agency electing to participate in today's framework; otherwise, such an agency could avoid such costs altogether by deciding not to participate in this information sharing. We find that the benefits attributable to providing NORS and DIRS access to these agencies and other parties are substantial and may have significant positive effects on the abilities of these entities to safeguard the health and safety of residents during times of natural disaster or other unanticipated events that impair telecommunications infrastructure.

55. Moreover, we are unaware of any alternative approaches with lower costs, nor have any been identified by commenters, that would still ensure that the Commission promptly and reliably learns of the actions described above that may lead to the disclosure of NORS or DIRS-related information. Lessening the promptness or reliability of notifications to the Commission would disincentivize providers from supplying robust and fulsome NORS and DIRS reports and therefore reduce the benefits that those filings would provide to the Commission and participating agencies alike. We find that this reduction in benefits would outweigh the expected modest cost savings to those participating agencies that would be required to provide notifications under the framework we adopt today.

E. Preemption and its Relation to State, Federal and Other Reporting Requirements

56. We reject requests from commenters that urge the Commission to preempt state outage reporting requirements. Some industry commenters, including T-Mobile and CenturyLink, generally favor preemption as they believe it will, among other considerations, promote uniformity in the outage reporting requirements they must observe. For example, T-Mobile states that ''[c]onsistent with its recognition that there should be consistency with regard to outage information available to the public, the Commission should preempt state laws requiring the submission of outage data by wireless carriers. These laws often establish different thresholds for trigging outage reporting and could cause public confusion.'' CenturyLink also comments that ''[a]pproximately 34 states have outage reporting requirements that, in most cases, do not align with the FCC's reporting criteria. Complying with these various state rules poses both a resource burden and a systems burden that would lack a corresponding benefit if states obtain outage information by accessing NORS/DIRS.''

57. We note that the actions we take today would not place any new NORS, DIRS or state-level filing requirements on service providers and we find no compelling reasons to upset our information sharing framework by implementing any additional requirements for service providers at this time. We further agree with the California Public Utilities Commission that ''preemption is not an issue in the *FNPRM,*'' and acknowledge that because the Commission did not seek comment on this issue, the record on this significant Federalism question is not fully developed. Nothing in this paragraph is intended to narrow limit, or broaden a party's opportunity to seek redress under all applicable existing laws, including through declaratory judgement in accordance with 47 CFR 1.2 of or rules, on grounds that a state rule or law is allegedly preempted by Federal law or rule, including our part 4 outage reporting rules. Such rights remain undisturbed by today's Order. As we have indicated above, we did not seek comment on the issue of preemption in this proceeding, and the record here is insufficient to make any determinations on a need to launch further proceedings on this issue. For this reason, we also agree with the California Governor's Office of Emergency Services that ''the FCC should decline any invitation to broadly preempt state law because the question is outside the scope of the present proceeding.'' Moreover, the Commission is persuaded by commenters, including NASUCA, NARUC and California Governor's Office of Emergency Services, underscoring that, currently, states can determine what outage reporting requirements are most appropriate for their jurisdictions.

F. Safeguards for Direct Access to NORS and DIRS Filings

58. We adopt specific safeguards to ensure the continued confidentiality, appropriate sharing, and limited disclosure of NORS and DIRS information. These safeguards include providing read-only access to NORS and DIRS filings, limiting the number of users with access to NORS and DIRS filings at participating agencies, requiring participating agencies to receive training on their privileges and obligations under the framework (such as reporting any known or reasonably suspected breach of protocol to the Commission and service providers), and potentially terminating access to agencies that misuse or improperly disclose NORS and DIRS data.

59. As several record commenters express overall concerns about adequately securing NORS and DIRS information, our safeguards strategically respond to potential NORS and DIRS data security threats. For example, our training requirements are intended to set clear parameters for how agencies use NORS and DIRS filings, our limits on agency user accounts will help us control account access, and our measures to audit account access will enable us to detect and quickly investigate potential misuse. We expect that, collectively, these safeguards will protect the NORS and DIRS data we will share under our framework from inappropriate use and minimize the potential harm from data breaches as noted by certain record commenters. Based on our review of the record, we find that the safeguards we adopt today appropriately balance the need to preserve the confidentiality of NORS and DIRS information against the need to provide agencies with critical information to assist them with protecting public safety.

1. Read-Only Direct Access to NORS and DIRS and Limits on Access to Historical Filings

60. In the *Second Further Notice,* the Commission renewed the Commission's proposal, first made in the *2016 Report and Order and Further Notice,* that participating state and Federal agencies

be granted direct access to NORS and DIRS filings in a read-only manner to help prevent the improper manipulation of NORS and DIRS data. We now adopt this proposal, finding that this approach is vital to protecting NORS and DIRS filings from improper use. We observe that all industry, public safety organizations, and state and local government parties commenting on the Commission's read-only proposal agree with it, with some specifically noting that they believe it will be an effective safeguard against the improper manipulation of NORS and DIRS data. Further, ATIS states that it strongly supports read-only access as a means ''to further enhance confidentiality.'' We agree with commenters that granting read-only access will help reduce the risk that participating agencies' employees or others could make unauthorized modifications to the filings, whether unintentional or malicious, and ensure the accuracy of information shared via the information sharing framework.

61. Some commenters encourage the Commission to implement additional technological measures to prevent the improper use of information, including mechanisms to limit the manipulation and improper access of printouts and downloadable NORS and DIRS data, such as placing confidentiality notifications or headers and watermarks on viewable and printable documents. We acknowledge that these recommendations would serve as useful safeguards against the improper use of outage data and find it would be in the public interest to further develop the record on the suitability of these measures and safeguards. We thus direct PSHSB to seek, via Public Notice, further information on the cost, manner and technical feasibility of implementing these technological measures and safeguards in NORS and DIRS and to make determinations on which of these measures and safeguards, if any, would be suitable for implementation in NORS and DIRS. We further delegate authority to PSHSB to implement in NORS and DIRS any measures and safeguards that it determines suitable and in the public interest based on the record developed in response to the Public Notice. Cognizant of the effective date of today's rules, we instruct the Bureau to work expeditiously to make its determinations and, if applicable, the associated revised implementations to NORS and DIRS. These implementations should not impose new regulatory requirements on service providers or additional conditions on agencies seeking access to the outage data. Nothing in this paragraph will serve as basis for delaying the effective date of the rules we adopt today.

62. The Commission also acknowledges the proposal from the Massachusetts Department of Telecommunications and Cable that the Commission ''establish a mechanism for Authorized State Agencies to comment on and give feedback to the FCC on the shared data,'' as the Massachusetts Department of Telecommunications and Cable believes that ''states may have information that does not appear in or that contradicts NORS or DIRS data, information which could allow the FCC to improve its data collection.'' We find that it is premature to determine whether this would be a useful feature for participating agencies, and we believe it is appropriate to wait until these agencies have had experience with NORS and DIRS before building this functionality into those systems. We suggest that participating agencies that wish to share information related to contents of NORS and DIRS filings instead informally contact Commission staff with their concerns.

63. *Access to Historical Filings.* The Commission proposed in the *Second Further Notice* to grant participating agencies access only to those NORS and DIRS filings made after the effective date of this proposed information sharing framework, even if the agency begins its participation at a later date. We adopt this approach today.

64. We are persuaded by industry commenters who argue that the Commission should not make available NORS and DIRS filings submitted before the effective date of the framework because the Commission should honor the expectation of confidentiality that providers had at the time they submitted them. For example, NTCA asserts that ''providers submitted their NORS and DIRS filings with the expectation that only the Commission would have access to those filings.'' We agree, and believe it would be inappropriate in this context to adopt rules to allow retroactive carte blanche access to these filings by agencies joining the framework as providers had no notice that we would share such confidential information with participating agencies and maintained an expectation that we would withhold them from disclosure. We also find that providing access to filings submitted before the effective date of the proposal would be technically difficult to implement, as it would require the modification of tens of thousands of previously filed outage reports to ensure that access can be limited by jurisdiction. Nonetheless, while we decline to adopt proposals to share filings submitted before the effective date of the framework, we also agree with public safety and state government commenters that having access to past filings could help identify trends in outages and be useful to agencies in planning and responding to outages to improve network reliability, and we reject industry commenters like CenturyLink, that argue to the contrary. On balance, however, we find that the need to preserve the confidentiality of filings submitted before the effective date of the framework is stronger than any rationale posited to support access to these filings. We believe that providing participating agencies with direct access to filings submitted after the effective date of the framework, even if their participation begins at a later date, is the optimal approach as it provides fair notice to service providers while also providing agencies with information to assist them with identifying outage trends over time and enhance their preparedness and recovery efforts as noted above and in the *Second Further Notice.*

65. We further note that ATIS argues that it ''does not believe that it is necessary to provide access to filings made before a state has been granted access,'' but ''should access to prior reports be made available,'' access to past reports should be limited to ''no earlier than 90 days,'' and ATIS proposes that should additional NORS and DIRS data be needed by participating agencies, the Commission could grant it ''upon a showing of reasonable necessity. We reject ATIS's argument as we do not find that ATIS provides a compelling explanation regarding why limiting access to reports to no earlier than 90 days is an appropriate window (as opposed to another window of time). Moreover, the Commission does not find any harm in sharing filings older than 90 days so long as they were made after the effective date of the framework, consistent with our decision today, as filers would be on notice of the prospect that their filings could become available to states that subsequently demonstrate their eligibility for access. The Commission also finds that requiring participating agencies to demonstrate a reasonable necessity for additional NORS and DIRS reports, as ATIS suggests, could impede efficient access to available NORS and DIRS filings.

2. Disclosing Aggregated NORS and DIRS Information

66. In the *Second Further Notice,* the Commission proposed to allow

participating agencies to provide aggregated NORS and DIRS information to any entity including the broader public. In doing so, ''aggregated NORS and DIRS information'' was defined to refer to information from the NORS and DIRS filings of at least four service providers that has been aggregated and anonymized to avoid identifying any service providers by name or in substance.'' The *Second Further Notice* articulated several potential public safety benefits stemming from the public disclosure of aggregated NORS and DIRS information, including its use in keeping the ''public informed of ongoing emergency and network outage situations, timelines for recovery, and geographic areas to avoid while disaster and emergency events are ongoing.''

67. Based on our review of the record, we continue to expect that the Commission's proposal will yield these benefits and adopt it today. We agree with commenters that assert that appropriate use of aggregation can provide useful information to public safety entities and the public while still maintaining the confidentiality of data submitted by providers.'' We disagree that agencies should be permitted to publicly disclose NORS and DIRS data that are not aggregated and anonymized as proposed, and accordingly, the rules we adopt today do not permit data to be treated as disclosable under the definition of ''aggregated NORS and DIRS information'' unless the data has been drawn from at least four service providers. Based on our experience in determining whether aggregated disclosure is appropriate in other contexts, we believe that where there are fewer than four service providers, the disclosure of aggregated outage information, particularly in combination with providers' specific knowledge of competitors in the region, could inadvertently reveal one service provider's commercially sensitive information to another. Even where the data is aggregated from four service providers, however, under the approach to disclosure we adopt today, agencies are prohibited from publicly disclosing such data if they cannot ensure that no one can derive the information of any individual company from the aggregation. For example, aggregating the data from four service providers may not sufficiently anonymize the data if one provider's data constitutes an overwhelming share of the total.

68. To help mitigate concerns regarding improper aggregation due to lack of expertise, we include exemplar aggregated and anonymized reports based on hypothetical data in Appendix D. This Appendix also contains non-binding guidelines for aggregating NORS and DIRS data. We expect this Appendix will show participating agencies how to aggregate users and cell sites affected by outages from NORS and DIRS reports in a manner that ensures anonymization to prevent misuse and address any potential confusion participating agencies have about aggregating NORS and DIRS data. As stated in this Appendix, we note that aggregated data may not reflect the exact number of users affected by a service provider's outage and is only used for situational awareness, and agencies' failure to properly aggregate data could lead to the improper disclosure of service providers' confidential information and may result in termination of their access to NORS and DIRS filings by the Commission. We believe that with the guidance we provide agencies today, they will be able to aggregate and anonymize NORS and DIRS data in accordance with our rules.

69. Several commenters have urged the Commission to adopt a broader definition of aggregation to enable aggregation in what they have described as the numerous areas that have fewer than four providers. For example, the California Public Utilities Commission comments that the ''proposal fails to consider aggregation in the many instances where an area is only served by two major wireline service providers.'' Allowing the public dissemination of NORS and DIRS information where there are only two providers, for example, however, would unnecessarily reveal confidential information about each of those providers to the other. We believe that the dangers posed by such disclosure substantially outweigh the benefits of disclosure to the public, given the availability of the data to participating agencies. We recognize that an agency's ability to provide aggregated information may depend on the types (*e.g.,* wireless or wireline) and numbers of providers serving a region and the unique circumstances of an outage; there, however, aggregated disclosure may be possible without an unauthorized disclosure of confidential information given the multiple providers of each type and at least four providers overall. Even so, there may be situations where, for an example, an outage affects only the two wireline providers in an area, and not the two wireless providers. In that case, only the two wireline providers would be filing reports, and any aggregation of their data would fall short of the four-or-more provider requirement for public disclosure. We find that this approach is necessary to ensure the confidentiality of NORS and DIRS information and strikes a reasonable balance between the relevant policy considerations. This policy does not override agreements certain wireless providers have made with the Commission regarding the use of aggregated DIRS data consistent with the Wireless Network Resiliency Cooperative Framework.

70. We reject one commenter's proposal that, if aggregated data may not be disclosed because of an insufficient number of providers, then the Commission should first conduct a ''risk assessment'' to determine how adversely affected the public would be by not receiving such data, and second, if the risk assessment shows harm, then the Commission should modify its ''need to know'' approach by disclosing information under a protective order to ''public safety officials, researchers, and public interest representatives.'' As a threshold matter, it is unclear what this commenter means by ''risk assessment,'' what specific metrics this commenter believes the ''risk assessment'' would use to measure what it refers to as ''the impact of disparate access,'' and what costs are associated with such an assessment to the Commission. To the extent this commenter is suggesting that such a risk assessment be used to identify parties that would qualify under the ''need-to-know'' standard as recipients of confidential information, we believe it is more appropriate to rely on state agencies to employ our new rules to share outage information downstream to the extent necessary to address an emergency situation for all affected within the community. We anticipate that, in the appropriate circumstances, public safety officials downstream from a participating state agency might have a ''need to know'' and may thus obtain confidential outage information from such an agency that has determined it permissible under our rules to share such information in this manner. It is perhaps less likely, however, that public interest organizations or researchers would qualify for such sharing under our rules. Insofar as this commenter would have us relax the ''need-to know'' requirements to allow such expanded sharing, we reject that proposal, as we believe that the balance we have struck between disclosure of some information to facilitate localized responses to emergencies and service outages caused by them, on the one hand, and the protection of sensitive data from unnecessary disclosure, on the other, will best serve the overall public

interest. We also note that no commenter has recommended a practical alternative to the Commission's proposal that would enable aggregation at a lower threshold while ensuring that national security and competitive concerns are addressed. Additionally, we note that under the Commission's proposal, participating agencies in areas with fewer than four communications providers have access to this data for public safety purposes consistent with the rules we adopt today; they simply may not disclose the data publicly.

71. ATIS and SIA argue that the Commission, instead of participating agencies, should produce or approve aggregated reports for public dissemination consistent with its existing practices and because of the Commission's expertise with issuing these reports. We reject these proposals. As dozens—or hundreds—of agencies might participate in the information sharing framework, and there could be several potential emergencies, and the need for prompt resolution of those emergencies and related outages, we find that it would be impractical and administratively burdensome for the Commission to produce aggregated and anonymized reports on behalf of all participating agencies seeking to publicly disseminate aggregated reports under the Commission's proposal.

72. We note that T-Mobile also contends that aggregated data should be disclosed only by the Commission because, among other considerations, ''public disclosure by agencies other than the FCC could ultimately mislead or confuse the public'' during times of crises. T-Mobile asserts that agencies' unfamiliarity with the data can lead to agencies either misinterpreting the data or producing aggregated data reports that differ from each other, and that ''these disparate reports would most likely cause confusion and potentially hinder, rather than help, situational awareness.'' T-Mobile further argues that as an alternative, the Commission should share data it already aggregates, such as the aggregated DIRS reports it publishes on its website. We reject T-Mobile's arguments. We find that, like the Commission, participating agencies with a ''need to know'' have or will quickly develop the necessary expertise to be able to understand NORS and DIRS information, coordinate with the Commission and regional partners where necessary, and release information to the public in a responsible way. For example, while NORS and DIRS filings often estimate the potential impact of service disruptions rather than reflect the exact number of users affected by an outage, those estimates can still effectively inform the public's understanding about the effect outages across several providers following a disaster and we expect that participating agencies will be able to communicate that information to the public in a productive way.

73. We do not agree that existing Commission data aggregations can replace state and local agencies' needs to inform the public about outages and infrastructure status. For example, we anticipate that some agencies will determine it is appropriate to release information to the public more frequently than once a day or in specific regions not covered by the Commission's public DIRS reports or any aggregations of outage data that it might prepare. Also, as we stated above, we believe that it would be impractical and administratively burdensome for the Commission itself to fulfill requests to aggregate NORS and DIRS data from potentially numerous participating agencies, and such an approach could delay the Commission's assistance with resolution of the underlying emergencies prompting the need to share the reports. To the extent that the Commission identifies any instances of an agency using NORS or DIRS information in an improper way, it will take steps to ensure that improper disclosure does not occur in the future.

3. Direct Access to NORS and DIRS Filings Based on Jurisdiction

74. In the *Second Further Notice,* the Commission acknowledged that outages and disasters can cross multiple jurisdictional boundaries and therefore proposed enabling a participating agency to receive direct access to all NORS notifications, initial reports, and final reports and all DIRS filings for events reported to occur at least partially in their jurisdiction including multistate outages. We also proposed enabling participating agencies to receive access to NORS and DIRS filings for outage events and disasters that occur in portions of their jurisdictions but also span across additional states. We sought comment on, *inter alia,* whether participating agencies would make use of NORS and DIRS filings that affect states beyond their own, whether participating agencies have a ''need to know'' about the effects of multistate outages and infrastructure status outside their jurisdiction, and whether any harms could potentially arise from granting a participating agency access to multistate outage and infrastructure information.

75. We adopt these proposals today as we expect they will enhance public safety by providing agencies with thorough information regarding outages to aid in their response and recovery coordination efforts. Several public safety and state government commenters support granting participating agencies multistate outage information about outages occurring at least partially in their jurisdictions. We agree with these commenters that access to this information would ensure that participating agencies have a complete picture of outages and their causes and would improve coordination between jurisdictions in response to disasters. We also agree with the Pennsylvania Public Utility Commission that participating agencies are ultimately in the best position to determine what effects of multistate outages and infrastructure status outside their jurisdiction are relevant to informing their responses to the event.

76. We disagree with commenters that argue that state access should be restricted to outage reports for those portions of events occurring in that state. For example, the Competitive Carriers Association contends that ''any decision to allow access to information about adjacent states should be made on a case-by-case basis only upon a showing of need,'' as it believes ''such geographic limitation is an important mechanism for the Commission to ensure that data is used only for intended purposes.'' We find that participating agencies would be better able to address public safety matters, including by improving their outreach and coordination with other jurisdictions in response to disasters, if they have a more complete picture of outages and their causes. ATIS further urges the Commission to prohibit the sharing of data from multistate events with agencies until it addresses how to effectuate this change in NORS. We also find that modifying NORS forms to allow users to select more than one state when submitting a NORS filing, as discussed further below, will be adequate to allow the Commission to ensure that participating agencies can only access filings for outages that at occur least partially in their jurisdiction.

77. *Sharing of Complete NORS and DIRS Reports and Filings.* In their comments concerning the scope and type of confidential information that should be shared with participating agencies, some industry commenters opine that some reports and fields in NORS and DIRS, such as root cause analyses, sympathy reports, reports on simplex events, contact information, and equipment types, are irrelevant and likely to cause confusion and contain confidential information. ATIS also

states information regarding ''special offices and facilities in Telecommunications Service Priorities (TSP) 1 and 2'' in NORS filings ''provide no relevant public safety information and should therefore not be shared with state agencies.'' A sympathy report contains information regarding a service outage that was caused by a failure in the network of another company. A simplex report contains information about which diversity of resources prevented a failure in a network from causing a loss of service. TSP is an FCC program that directs telecommunications service providers to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. In NORS, providers can indicate if TSP was involved during service restoration. A root cause analysis indicates the underlying reason why the outage occurred or why the outage was reportable. CTIA and Verizon recommend the Commission convene a workshop to discuss practices for inter-jurisdictional sharing of information, which USTelecom supports as a way to determine what information is necessary to share.

78. On review, we reject most commenters' proposals to share only certain types of outage filings made in NORS and DIRS and reject proposals to convene workshops to identify the appropriate types of NORS and DIRS data to share. We agree with ATIS that reports related to simplex events as contained in NORS filings should not be shared with participating agencies. These reports contain information that helps identify which diversity of resources prevented a failure in a network from causing a loss of service, which could be helpful for analyzing trends in outages, but we find that this information is not immediately relevant to emergency response. However, we note that sympathy reports and reports containing information about TSPs contain actionable information on outages that could be of use to public safety officials for emergency response or service restoration and we decline to exclude these reports from NORS filings. For example, sympathy reports contain information regarding service outages that, while caused by a failure in the network of another provider, nonetheless have an effect on the reporting service provider that may have public safety implications. Moreover, information about TSPs may be helpful to emergency response officials to indicate which repairs are being prioritized by service providers.

79. For the NORS filings that are shared with participating agencies, including notifications, initial and final reports, we find that their contents about service outages, such as dates and times of incidents, geographic areas affected, effects of outages on 911 service, the numbers of potentially affected users, and causes (including information about any affected equipment) are highly relevant to agencies that seek to increase their situational awareness of emergency events and coordinate disaster response and recovery efforts. Furthermore, in response to several commenters' position that some fields in NORS reports are too sensitive or confusing to share and should be excluded, we expect participating agencies will be able to discern which information from various types of NORS and DIRS filings is relevant to their own circumstances during various stages of public safety events, particularly as we expect that participating agencies will possess sufficient technical and operational expertise to understand the information that some commenters maintain could be confusing. We also find that the confidentiality requirements and safeguards we adopt today will protect sensitive NORS information from improper use and disclosure. We recognize that, once the information sharing framework becomes effective, participating agencies may initially engage the Commission (and potentially service providers, through their existing relationships) with questions about NORS and DIRS data, which will lead to more effective use of all types NORS and DIRS filings over time.

80. We specifically reject the view that all of a service providers' contact information should be excluded in the NORS and DIRS filings and information we share with participating agencies. As noted by the Michigan Public Service Commission, we expect that agencies' technical staff will review NORS and DIRS filings and that the staff will occasionally require contact with providers experiencing outages in their jurisdiction to better understand and resolve substantive issues. Because we expect that agencies will analyze NORS and DIRS information in similar ways to the Commission, we disagree with ATIS's view that all contact information supplied to the Commission with a filing should be excluded from sharing. However, we agree with commenters that it is unnecessary to share with participating agencies the contact information of those individuals that solely file NORS or DIRS information and do not have substantive details to share about an outage or infrastructure status. We find that this approach strikes an appropriate balance between ensuring participating agencies have access to the substantive information they need and avoiding unproductive contact that can potentially distract from the making of timely filings. We note that, currently, NORS and DIRS give providers the option to list primary (or first) and secondary contacts, either for an outage (NORS) or generally for the provider (DIRS). We clarify that the providers should enter as their primary contact an individual that they specifically designate for substantive follow-up discussion about an outage or about infrastructure status. For the secondary contact, providers should identify the individual who undertakes the administrative task of preparing and filing applicable reports in NORS and DIRS. By following this guidance, providers can help ensure consistency in the communications between themselves and participating agencies.

81. *Tribal Nation Government Agency/State Agency Access to Multistate Event Data.* In the *Second Further Notice,* the Commission asked whether a participating Federally recognized Tribal Nation agency that receives direct access to NORS and DIRS filings has a ''need to know'' about events that occur entirely outside of its borders but within the border of the state where the Tribal land is located, or if a state agency should ''receive direct access to NORS and DIRS filings reflecting events occurring entirely within Tribal land located in the state's boundaries. The Commission further asked whether any harms could ''arise from granting Tribal Nation authorities access to outage and infrastructure information outside of their territories,'' and sought comment on whether ''Tribal Nation authorities' access to NORS and DIRS filings should be limited only to those aspects of multistate outages that occur solely in their territories.''

82. NASNA and the Colorado Public Utilities Commission, the only two commenters opining specifically on this issue, both agree that a Federally recognized Tribal Nation agency that receives direct access to NORS and DIRS filings can have a 'need to know' about events that occur entirely outside of its borders but within the border of the state where the Tribal land is located. We are persuaded by NASNA and the Colorado Public Utilities Commission's comments and note that no commenter opposes this approach. We adopt the proposal that a Federally recognized Tribal Nation agency may

receive direct access to NORS and DIRS filings for events that occur entirely outside of its borders but within the borders of the state where the Tribal land is located and, conversely, that a state agency receive direct access to these filings reflecting events occurring entirely within Tribal land located in the state's boundaries to the extent these filings are available, and access would not impinge upon Tribal sovereignty. We also grant Tribal Nation agencies direct access to NORS and DIRS filings for outage events and disasters that occur in portions of their jurisdictions but also span across additional states. As the Commission stated in the *Second Further Notice,* because of the technical nature of many outages, equipment located in a Tribal land could impact service in the states in which Tribal lands are located, and we expect this action to enhance the situational awareness of Tribal Nations, and the states in which they are located, regarding service outages and thereby improve public safety. We note that NASNA supports the Commission's proposal to give state agencies direct access to NORS and DIRS filings for events occurring entirely within Tribal land located in a state's boundaries to improve information sharing between states and Tribal nations. NASNA states that ''it would be most efficient to allow direct access to data that relates to incidents within a state agency's state boundaries, and to a tribal entity's tribal jurisdiction,'' and comments that this approach ''gives the states and tribal entities the ability to share data when it is appropriate.'' We note that this approach does not impact Tribal sovereignty as under our framework, outage data will be provided in the first instance by the provider to the FCC, and only thereafter shared with a Tribal entity.

83. *Technical Implementation.* In the *Second Further Notice,* the Commission sought comment on aspects of the technical implementation of its proposals regarding direct access to NORS and DIRS filings based on jurisdiction, including its assertion that service providers would incur minimal, if any, burdens related to DIRS because they would not need to modify their DIRS reporting processes to accommodate multistate reporting. The Commission also proposed changing the Commission's NORS form to allow users to select more than one state when submitting a NORS filing, consistent with the proposal to allow access to outages that span multiple states. The Commission estimated the cost of such a change for the nation's service providers to be $3.2 million and sought comment on this proposal and any potential alternatives, including any necessary adjustments to account for Tribal land borders. While a few commenters expressed concerns about the accuracy of estimated costs to service providers, no commenters provided cost data or analysis to support their concerns or rebut the Commission's cost estimates. Similarly, while some state agency and advocacy organizations expressed concerns that it will be burdensome for voluntarily participating agencies to relay information they retrieve from the NORS and DIRS databases to ''downstream'' entities, none of these entities attempt to quantify the costs associated with these activities. In the absence of any cost analyses or other cost data quantifying alternative cost estimates, the Commission continues to rely upon the estimates discussed in the *Second Further Notice* indicating that the nation's service providers will incur total initial set up costs of $3.2 million based on the Commission's estimate of 1,000 service provider incurring costs of $80 per hour and spending 40 hours to implement update or revise their software used to report outages to the Commission in NORS and DIRS.

84. We thus adopt this proposal consistent with our view that it will allow the Commission to effectuate our provision of access to filings for outages that span more than one state, and we conclude that the benefits of today's program far exceed the costs. We note that commenters did not address the Commission's assessment that service providers would likely incur minimal to no costs to accommodate DIRS reporting as DIRS form already requests filers to include data at the county level. However, most parties commenting on the Commission's proposed NORS modification support the NORS modification. For example, NCTA supports this approach because it allows the Commission to limit participating agencies' access to information about those outages that occur within their jurisdiction. Furthermore, CenturyLink states that also it prefers this approach, provided that the Commission does not require state-specific impacts to be broken out for each reported outage. This change in NORS reporting can be accomplished without revising section 4.2 of our rules as section 4.11 of our rules already requires that, *inter alia,* communications providers supply, in their NORS filings to the Commission, information on the geographic area affected by an outage using the Commission's approved Web-based outage reporting templates. Here, the Commission is merely updating the form of its templates to further facilitate jurisdiction-specific access.''

85. We note that NTCA ''recommends the Commission undertake a cost benefit analysis of any proposed changes to the method in which providers submit information into the NORS and DIRS systems to ensure any burdens imposed on providers caused by having to modify the way they report outages and any additional time needed to report outages to meet any new requirements are outweighed by the benefit to public safety.'' As we note above, we have performed this analysis and find that the changes we adopt today ensure that the burdens imposed on providers are outweighed by the public safety benefits of our information sharing framework. We further acknowledge commenters' proposals to include Tribal Nation agencies in the list of jurisdictions for providers to choose from in NORS. However, we decline to adopt these proposals because we find that it would be administratively burdensome and difficult to continuously track the full extent of existing Tribal Nation agencies to include and update in NORS. However, we note that the approach we adopt above, to give Tribal Nation agencies access to outage reports within the border of the state where the Tribal land is located, would achieve the same goals in a less burdensome manner.

86. Additionally, in the *Second Further Notice,* the Commission asked, as an alternative, whether it should require service providers to submit several state-specific filings instead of submitting single aggregated filings for each outage that list all affected states. All parties commenting on this issue disagree with this approach and assert that it would increase reporting burdens on service providers. NASNA notes that this proposal ''certainly seems less efficient and more time consuming for the providers than making the proposed change to the Commission's reporting form, but since the end result to the participating state agencies is the same, NASNA leaves it to the providers to express its preference on this matter.'' CoPUC's comments echo NASNA's on this issue. Based on our review of the record, we are persuaded by comments underscoring the burdens this approach would impose on service providers and, thus, we decline to adopt it.

4. Limiting the Number of User Accounts per Participating Agency

87. *Presumptive Limits on User Accounts.* In the *Second Further Notice,* the Commission proposed to presumptively limit the number of user

accounts granted to a participating agency to five accounts for NORS and DIRS access per state or Federal agency with additional accounts permitted on an agency's reasonable showing of need. Furthermore, to ''reduce the reliance of any one agency on another by allowing each to apply for direct access to NORS and DIRS filings,'' the Commission also proposed, in the *Second Further Notice,* that the Commission review all reasonable requests from state and Federal agencies, rather than proposing a presumptive limit on the number of participating agencies eligible for direct access to NORS and DIRS filings.

88. We adopt the Commission's proposals today as we find that that they will limit access to NORS and DIRS information to the employees that are intended to receive it and allow participating agencies to identify misuse by specific employees. Colorado Public Utilities Commission and NASNA recommend that the language of the Commission's proposal be clarified to read that ''access should be up to five employees per agency, not per state.'' We adopt this clarification today for precision. We note that the majority of record commenters support the Commission's proposal to presumptively limit the number of user accounts, underscoring the *Second Further Notice'*s assertion that it is an important safeguard to minimize the potential for over-disclosure of sensitive information. For example, ACA Connects notes that implementing this measure will ''limit the risk of improper use or disclosure of the data.'' However, we disagree with ATIS that we should ''better define what a 'reasonable showing of need' would entail'' for granting additional accounts to agencies. While some factors that we expect could help demonstrate a reasonable showing of need include the jurisdictional area that an agency serves or the number of public safety functions for which it is responsible, we decline to require or define specific factors and will decide all requests on a case-by-case basis.

89. NASNA and the Colorado Public Utilities Commission support the Commission's proposals to review all requests for direct access from eligible agencies and not to restrict the number of potentially participating agencies. Verizon argues that the ''Commission should adopt a presumption that two agencies within a state may have access to the reports,'' as it asserts this action ''would better reflect that most states maintain both a single regulatory commission with some public safety-related responsibilities and a statewide executive branch emergency management agency.'' Verizon further argues that the ''Commission would have discretion to expand this number upon a good faith showing as this governance structure may vary among states, but reducing the presumptive number would help incent different state agencies to coordinate their information gathering efforts in advance of major outage events.''

90. We reject Verizon's proposal that the Commission adopt a presumption that two agencies within a state may have access to NORS and DIRS filings. We expect that participating agencies will indicate, in their application for access, the legal authority that charges them with promoting the protection of life or property. This showing will allow us to best assess whether specific state agencies should have access to these filings. We also find that allowing only two entities to have access to NORS and DIRS filings could necessitate a competitive process to determine which agency would get selected, which would delay access, not have clear standards, and may lead to disharmony among agencies that need to coordinate and cooperate. Additionally, we find that granting access to all qualifying agencies will make each of those entities more accountable to the Commission as they would have to bind themselves to the program's requirements when signing the certification.

91. *Agency Assignment and Management of User Accounts.* The *Second Further Notice* proposed requiring that ''an agency assign each user account to a unique employee and manage the process of reassigning user accounts as its roster of employees changes.'' As we continue to find that these proposals will minimize the improper use of NORS and DIRS information and give participating agencies flexibility for managing user accounts, we adopt them with certain modifications to further strengthen our account management requirements. The Commission will retain for its records the unique account identifiers associated with each agency. We note that while ATIS specifically expresses support for the *Second Further Notice'*s proposal that agencies assign user accounts to employees and manage the reassignment process for these accounts, most commenters do not rebut the necessity of these proposals to protect against improper disclosure. However, some industry commenters propose placing additional limitations on agency access to prevent improper use, which we adopt or reject *infra.*

92. AT&T recommends the Commission designate a ''coordinator'' to be responsible for ''an agency's access to confidential NORS/DIRS information,'' as it believes this will ''ensure that each potential recipient has a 'need to know' basis for access to the information, the recipient understands the duty to maintain confidentiality, and the information will be destroyed in a secure manner when there is no longer a need to know.'' AT&T states that after designation ''the coordinator would have the ability to approve additional requests for access credentials for personnel from that agency,'' and that this ''approach would allow downstream sharing of information by the coordinator who would be best positioned to ensure that recipients have a 'need to know.' '' AT&T further argues that a ''similar procedure has worked well in the context of the 911 Reliability Certification System,'' and states that for that procedure, ''the potential information recipient sends a request to a designated FCC staff member to receive coordinator status and these requests are handled on case-by-case basis.'' No commenters oppose AT&T's recommendation.

93. We adopt AT&T's recommendation as we find that it would help facilitate the efficient administration of our framework and provide additional safeguards to protect NORS and DIRS data for the reasons it describes. Therefore, we will require participating agencies, in the Certification Form (Appendix C) we adopt today, to indicate the name and contact information of their agency coordinator. We will require this agency employee to serve as their agency's point of contact for all matters related to their agency's framework access, including managing agency accounts, submitting requests for additional user accounts, coordinating downstream sharing consistent with our rules, coordinating with the Commission to manage any unauthorized access incidents, and taking reasonable efforts to make available for Commission inspection a list of all localities for which the agency has disclosed NORS and DIRS data.

94. Several commenters recommend the implementation of auditing and reporting measures to minimize improper use. For example, ATIS recommends that ''the Commission require states to conduct an internal audit every six months . . . of individuals with access to determine whether these accounts are still necessary and to require personnel to regularly update passwords,'' and that ''the results of this audit should be shared with the Commission.'' CTIA recommends that the Commission ''develop a process for regularly

auditing accounts it has granted to public safety stakeholder agencies and sharing the results of this process with providers that file reports to NORS and DIRS.'' USTelecom proposes that the framework ''contain regular reports that provide a record of how many active accounts are maintained by each agency and the number of reports accessed by each,'' and that ''upon request, and in a reasonable time frame,'' the Commission ''provide reports to carriers listing which Federal or state government agency accounts have accessed their NORS or DIRS outage data.'' Moreover, NCTA recommends suspending ''individual user access if an individual has not accessed NORS or DIRS within a 12-month period.'' We reject all commenters' auditing and report production proposals as they would place undue obligations on the Commission and participating agencies and could be financially prohibitive. We further find that requiring the suspension of access to users that are inactive over 12 months is too prescriptive. For example, given the sporadic nature of disasters and emergency events, users at some participating agencies might not access NORS and DIRS filings for over a year.

95. Additionally, to increase account security, several parties make proposals that recommend the tracking of how users access NORS and DIRS filings. For instance, NTCA recommends requiring ''agencies accessing the filings to track the name of the authorized individual within the agency that accessed information and when.'' CTIA states that the ''Commission should ensure that adequate tools are available to aid investigations after data breaches,'' and opines that ''one such tool is an audit log for the NORS and DIRS database, recording which data was accessed, when, and by whom.'' NCTA recommends that ''reporting service providers should be able through online access to obtain information identifying both the agencies and the user accounts that accessed their information.'' We adopt CTIA's approach and will develop auditing capabilities into NORS and DIRS that track which reports specific users access and when they are accessed. We note that no commenters oppose this approach. We believe this will allow the Commission to maintain effective oversight as to how NORS and DIRS are used, including following an incident involving unauthorized access. We believe that this approach will be less burdensome on participating agencies than the approaches recommended by NTCA and NCTA, respectively. We acknowledge however the contentions of commenters who have argued that service providers should have access to these logs so that they can determine whether their data has been mishandled. We find that service providers have a legitimate interest in ensuring that their presumptively confidential data is handled appropriately even as we remain wary that service providers could use such information to burden participating agencies with queries based on the logs, particularly during times of exigency. Therefore, we delegate authority to PSHSB to consider written requests from service providers for access to audit logs regarding their own records on a case-by-case basis and to release requested information to the requesting service provider only if PSHSB determines that doing so would be in the public interest. A service provider's written request must explain the specific circumstances that the provider believes warrants its access to audit logs and identify, with particularity, the requested date ranges and entities covered by in the request.

5. Training Requirements

96. In the *Second Further Notice,* the Commission proposed that each individual granted a user account for direct access to NORS and DIRS filings be required to complete security training on the proper access, use of, and compliance with safeguards to protect these filings prior to being granted initial access, and that this training occur on an annual basis thereafter to make the framework more effective and reduce the risk of over-disclosure of NORS and DIRS information. Furthermore, the Commission sought comment on whether anyone who receives confidential NORS and DIRS information, including downstream recipients, be required to complete formal training. We adopt a proposed training requirement today, and note that an overwhelming number of commenters submit that some form of training is necessary for participating agencies to ensure the appropriate uses of NORS and DIRS data and minimize over-disclosure, and believe participating agencies should certify that they have undertaken security training consistent with the Commission's requirements. For example, the Public Service Commission of the District of Columbia opines that it ''agrees with the FCC and many commenters that training of authorized state agency staff about NORS and DIRS reporting is important to ensure proper treatment of NORS and DIRS information.'' The Competitive Carriers Association states that it ''supports the Commission's proposal to mandate annual security trainings to agency personnel accessing the data,'' and that ''considering the sensitive nature of NORS and DIRS data, regular security trainings will help ensure safeguards are adhered to and that information remains protected.''

97. We acknowledge that the Michigan Public Service Commission states that it ''does not support the proposal for annual training requirements as currently discussed in the FNPRM,'' as it contends that if ''there are to be annual certifications to access NORS and DIRS outage information, the MPSC believes that any required training should be free of charge to applicants and centrally located or made available online.'' The IACP also recommends that ''any required training be accessible on-line and be time limited to that which is necessary to cover the points required.'' As we decline to prescribe specific training or platforms that agencies must use to facilitate training, we respond to the Michigan Public Service Commission's concerns by noting that we expect that the implementation of our training requirements, as discussed below, will give agencies the opportunity to tailor training programs to their unique needs, including considerations of cost.

98. Furthermore, in the *Second Further Notice,* the Commission sought comment on whether anyone who receives confidential NORS and DIRS information, including downstream recipients, should be required to complete formal training. While we decline to adopt a formal training requirement for downstream recipients, we will require participating agencies to instruct downstream recipients to keep NORS and DIRS information they receive as confidential and obtain a certification from downstream entities that they will treat the information as confidential.

99. We note that commenters are divided on this issue. For example, while the Pennsylvania Public Utilities Commission and the Satellite Industry Association maintain that downstream training should be required to ensure that downstream recipients understand the consequences of downstream sharing and to reduce the risk of the mishandling of NORS and DIRS information. NASNA and the Colorado Public Utilities Commission disagree. For example, the Colorado Public Utilities Commission states that ''there are potentially hundreds of individual agencies throughout the state that may have a ''need to know'' during a disaster

or large-scale emergency, and requiring each of those agencies to have individuals undertake a multi-hour training prior to receiving the information is unreasonable,'' and further argues that it ''would also be unduly burdensome for the participating state agency to keep track of who has had training, who hasn't, and whether annual refresher training has been maintained.'' As an alternative to downstream training, the Colorado Public Utilities Commission and NASNA suggest that a participating agency ''be allowed to develop an affidavit to be signed by subrecipients prior to the receipt of confidential information, acknowledging that they understand that un-anonymized data is confidential and that it is not to be shared.''

100. We are persuaded by NASNA and the Colorado Public Utilities Commission's assertion that a downstream training requirement would be unreasonable, given the potentially hundreds of downstream entities that might receive information through the framework. However, we find that providing downstream access with insufficient safeguards could amplify the possibility of unauthorized disclosure, particularly because downstream entities will have less experience with protecting NORS and DIRS data than participating agencies. Therefore, we also agree with NASNA and the Colorado Public Utilities Commission's alternative approach.

101. We will require participating agencies sharing data with entities that have a ''need to know'' to instruct these entities that they must treat the information as confidential, not disclose it absent a finding by the Commission that allows it to do so, report any unauthorized access, and securely destroy the information when the public safety event that warrants its access to the information has concluded. We delegate authority to PSHSB to develop a certification for use by participating agencies. Furthermore, as we explain *infra,* we will hold participating agencies responsible for inappropriate disclosures of NORS and DIRS information by the non-participating agencies with which they share it. We will also require participating agencies to obtain non-participating agencies' certification, under the penalty of perjury, that they will abide by these restrictions.

102. We note that NTCA ''encourages the Commission to adopt rules requiring any local, state or Federal personnel with access to NORS and DIRS filings sign a certification attesting they have undertaken security training consistent with the Commission's recommendation . . . and will access and use the information only for the public safety purposes for which it is intended.'' We find that our downstream training requirements that we adopt today, along with the required Certification Form we discuss *infra,* provides for adequate training of personnel, enables us to obtain appropriate acknowledgment from agencies regarding their efforts to train employees on the appropriate uses of NORS and DIRS information. Consistent with NCTA's proposal, the Certification Form as described *infra* will require participating agencies granted access to certify that they have completed security training and will use NORS and DIRS information for public safety purposes only. However, we decline to adopt this requirement for local personnel through the Certification Form as we are not requiring training for downstream entities granted access to NORS and DIRS information by participating agencies, and we will require participating agencies to obtain a separate certification from these entities regarding the appropriate use of NORS and DIRS information as described above.

103. *Agency Compliance with Training Requirements.* In the *Second Further Notice,* the Commission sought comment on requiring third-party audits to ''ensure that state and Federal agencies' training programs comply with the Commission's proposed required program elements'' and asked ''what specific steps should the Commission take, if any, to ensure the adequacy of such programs.'' ATIS ''urges the Commission to consider reviewing and formally approving all training programs to ensure that they are effective and address all relevant issues.'' NASNA and the Colorado Public Utilities Commission believe that in lieu of requiring third-party audits of partner training programs, participating agencies should provide a copy of their training curriculum to the FCC. For example, NASNA states that if ''the FCC requires reassurance that participating agencies are meeting training requirements, those agencies could be required to provide a copy of its training curriculum to the FCC and attest that all employees within the agency are required to complete the training prior to applying for an account,'' and that the ''same requirement could exist for the annual refresher training requirement.''

104. We adopt a requirement, consistent with NASNA and the Colorado Public Utilities Commission's proposal, to require participating agencies to make copies of their training curriculum available for the Commission's review upon request. We are persuaded that is approach will be the most effective way for the Commission to confirm the adequacy of state and Federal training programs, and mandate remediation as necessary, without burdening participating agencies with a requirement to procure third-party audits. We will not require advance review and approval of agencies' training materials by the Commission, as we find that doing so would be administratively burdensome to the Commission and prevent efficient access to NORS and DIRS information. We also find that requiring advance review is unnecessary, as we believe that requiring agencies to certify to the adequacy of their training programs, as discussed *infra,* is sufficient to ensure that the plans' adequacy.

105. *Training Program Required Elements and Exemplars.* In the *Second Further Notice,* the Commission proposed that rather than mandating an agency's use of a specific training program, agencies ''develop their own training program or rely on an outside training program that covers, at a minimum, specific topics or ''program elements. These program elements are: ''(i) Procedures and requirements for accessing NORS and DIRS filings; (ii) parameters by which agency employees may share confidential and aggregated NORS and DIRS information; (iii) initial and continuing requirements to receive trainings; (iv) notification that failure to abide by the required program elements will result in personal or agency termination of access to NORS and DIRS filings and liability to service providers and third-parties under applicable state and Federal law; and (v) notification to the Commission, at its designated email address, concerning any questions, concerns, account management issues, reporting any known or reasonably suspected breach of protocol and, if needed, requesting service providers' contact information upon learning of a known or reasonably suspected breach.'' Additionally, the Commission proposed ''that [it] direct PSHSB to identify one or more exemplar training programs which would satisfy the required program elements.'' We adopt these proposals today with slight modifications as we continue to find that they are critical to ensuring participating agencies' comprehensive understanding of our information sharing framework. Specifically, we adopt a requirement that participating agencies' training programs must cover the five program elements that the Commission identified in the *Second Further Notice;* we enable agencies to

develop their own training program or rely on an outside training program that includes these program elements; and delegate authority to PSHSB the duty to consult with diverse stakeholders to identify an exemplar training program or develop exemplar training materials that include these program elements.

106. We observe that ATIS, the only commenter specifically addressing the proposed training program's required elements, supports those elements. Moreover, some commenters underscore their belief that to help facilitate uniformity of training materials and reduce burdens on participating agencies, the Commission should identify exemplar training programs that participating agencies can use in their efforts to train staff on the proper uses of NORS and DIRS filings.

107. The *Second Further Notice* also sought comment on ''the benefits and drawbacks to the Commission potentially working with one or more external partners, such as ATIS, to develop exemplar training programs.'' ATIS states that it would ''be happy to assist with development of a training program,'' and would ''work collaboratively with other associations so that this training would be completed within a reasonable time after the release of the final rules.'' The Boulder Regional Emergency Telephone Service Authority urges ''the Commission to decline the ATIS's offer to develop training which ATIS proposes to focus solely on limitations on use of the materials and penalties for misuse,'' because it believes that ''training should'' ''focus on interpretation and utility of data.'' Verizon states that training for the confidentiality requirements it recommends ''would be appropriate, in coordination with Commission staff, ATIS and public safety stakeholders.'' Verizon also states that the framework safeguards it supports in its comments ''should be another subject of the workshops it recommends.''

108. We find that many stakeholders, including ATIS, possess significant technical and operational expertise that could benefit the Commission in the development of exemplar training. Thus, to identify an exemplar training program or develop exemplar training materials, the Commission delegates authority to PSHSB to consult with diverse stakeholders with a range of perspectives, including state governments, the public safety community, service providers, and other industry representatives. We find that this approach will foster a collaborative process to ensure training materials reflect the needs of all information sharing framework participants. We note that ATIS also recommends that the training specifically provide guidance on six specific guidance topics. These topics are ''(1) The purpose of NORS and DIRS; (2) Appropriate use of confidential and aggregated data; (3) Who would be deemed to have a ''need to know;'' (4) What would qualify as a public safety purpose; (5) Proper distribution and use of printouts, including a requirement that users not delete the notification proposed by ATIS informing readers that the information in the document may be shared only with authorized users with a ''need to know,'' only for public safety purposes, etc.; and (6) The requirement that, should there be a known or suspect breach as noted above, the party whose data was breached must be immediately notified.'' We decline to adopt these recommendations at this time but note that ATIS has the opportunity to recommend these specific guidance topics if it works with the Commission and other stakeholders to develop exemplar training materials.

109. Some commenters also suggest the Commission convene stakeholder workshops, or facilitate other collaborative measures, before initiating the sharing framework to further develop data sharing protocol and other features of the framework as necessary. For instance, Verizon contends that ''to ensure that any new rules are implemented collaboratively among the service providers and government agencies involved, the Commission should convene stakeholder workshops in the months preceding adoption of final rules.'' Several other commenters support workshops' proposals. According to Verizon, these workshops could allow stakeholders to, in part, ''work through IT implementation challenges to ensure compatibility with providers' and state agencies systems,'' ''establish practices and guidance for permissible uses and sharing of information with employees and local government stakeholders,'' and ''help educate state and local governments on the information *not* included in NORS and DIRS reports, and on how service providers obtain information to include in the reports.'' Verizon further opines that to establish practices for downstream sharing and use of information, the Commission could initiate ''workshops of its own'' and encourage ''other collaborative discussions involving industry and public safety trade associations and standards groups,'' and incorporate ''those practices into training.'' CTIA also argues that ''the Commission should convene a broad group of subject matter experts to identify processes to protect data confidentiality while advancing outage information sharing with public safety stakeholders.'' Furthermore, AT&T recommends that ''before initiating agency and public disclosures, the Commission should give providers and government agencies the opportunity to review an example of the information to be made available through this process,'' and states that ''[i]t would be useful for the providers that submit information to NORS/DIRS to see a mock-up format, any template, and online access tools to be used so that they have an opportunity to raise any concerns and recommend changes.'' AT&T also states that ''[s]imilarly, feedback from government agencies would ensure that the Commission's final framework provides the state-specific information sought by these parties, while potentially minimizing multiple operationally redundant reporting regimes across providers' service footprints,'' and ''[s]uch a collaborative process is most likely to achieve the Commission's dual purposes of giving government agencies useful information while also preserving confidentiality of sensitive data.

110. We find that workshops are not an appropriate venue to develop requirements for our framework as the open record has provided all interested parties with an opportunity to comment on our, and other parties', proposals in this proceeding. Thus, we reject all recommendations that workshops be used, in any way, to develop our framework rules, including rules regarding downstream and inter-jurisdictional sharing. We further reject AT&T's proposal to enable providers and participating agencies to review and provide feedback on information to be made available through the framework before its initiation. We expect that the exemplar training materials supplied to agencies, which will be developed with the input of diverse stakeholders, will provide information to help guide agencies on the proper ways to access and use NORS and DIRS information, which they can choose to integrate into any training materials they develop. However, we delegate authority to PSHSB to host one or more workshops before the effective date of the framework to educate stakeholders about NORS and DIRS filings generally and the requirements we adopt today, including our rules regarding the appropriate uses of NORS and DIRS data, training measures, and aspects of IT implementation of the framework.

6. Sharing of Confidential NORS and DIRS Information

111. *Responsibilities of Participating Agencies.* In the *Second Further Notice,* the Commission proposed to allow individuals granted credentials for direct access to NORS and DIRS filings to share copies of the filings, in whole or part, and any confidential information derived from the filings within their agency, on a strict ''need to know'' basis. We adopt this proposal.

112. Commenters generally support allowing individuals with direct access credentials at a participating agency to share confidential NORS and DIRS information with individuals within their agencies on a ''need to know'' basis. We agree with the Pennsylvania Public Utility Commission that this mechanism is especially important given the many individuals involved in coordinating emergency response, many of whom will not be credentialed for access, and we agree with T-Mobile that it is prudent to ensure that non-participating agency officials are able to receive NORS and DIRS information to steer their agency in improving public safety outcomes. Moreover, we find the proposed approach to be a practical way to enable the individuals who are credentialed to login to our databases and thereby access NORS and DIRS filings to convey this filed information to their agency's decision makers. We find significant public safety benefits in ensuring that all ''need to know'' individuals at any agency, including key executives, decision-makers and potentially first responders, have access to NORS and DIRS information and we find this will allow an agency to make collectively informed decisions on how to use the information, ultimately lowering rather than increasing the chance of misuse of the information.

113. We reject CTIA's contrasting view that restricting access to credentialed users at an agency is a necessary safeguard for encouraging service providers to provide robust disclosures of relevant information in their NORS and DIRS filings. To the contrary, we find that if credentialed users could not coordinate with non-credentialed decision-making officials and other expert agency personnel on the substance of NORS and DIRS reports, this would likely lead to more instances of impermissible use and improper disclosure (and worse public safety outcomes), rather than fewer instances. For example, if a credentialed user cannot share NORS and DIRS information with specialized emergency management experts within their own agency, they would potentially use the information to make recommendations on public safety matters that they are not qualified to make. If a credentialed user cannot share NORS and DIRS information with agency decision-makers, they would potentially make decisions on allocating resources in response to a public safety threat that they would not have the authority to make. We find that the risks of improper disclosure would increase as credentialed users would be forced to work outside of their agency's normal chain of command in acting on confidential NORS and DIRS information. We believe that service providers will recognize that this observation, along the many safeguards implemented today, provide assurances the presumptively confidential NORS and DIRS filings the supply to the Commission will continue to be protected, and we believe that service providers will remain motivated in supplying robust NORS and DIRS filings to resolve network reliability and outage issues, as they have historically done. We note that service providers are required to submit NORS reports that meet all the requirements of our part 4 rules. While DIRS reporting is voluntary, our experience with DIRS activations provides us with the insight that providers are likely to provide complete DIRS reports in order to take advantage of the Commission's waiver of the NORS reporting obligations in those regions where DIRS has been activated.

114. We are also unpersuaded by NCTA's concern that ''increasing the number of people who have access to the data inherently increases the risk of breach or accidental disclosure'' because this conceptual possibility of an increased risk is outweighed by the harms that arise from disallowing intra-agency sharing, which would make it less likely that an agency's staff and leadership will use NORS and DIRS information to take action, thereby frustrating the purposes of the information sharing framework we adopt today.

115. Based on concerns of commenters, we bar the sharing of confidential NORS and DIRS information with contractors. While we recognize that an agency's contractors can engage in public safety functions in times of crises, we find that sharing with contractors should be barred given the potential for conflicts of interest among contractors, who may work on behalf of service providers as well as public safety agencies. As no commenter has identified how NORS and DIRS information can be shared in ways that would appropriately address these potential conflicts of interest, we decline to make this information available to contractors.

116. With respect to a participating agency's sharing of reports with downstream entities (described *infra*), in the *Second Further Notice,* the Commission proposed that the sharing agency determine whether a ''need to know'' exists on the part of the recipient. We adopt this proposal, which most commenters support without significant comment. With regard to potential costs burdens, we reiterate that participating agencies are not required to share NORS and DIRS information but instead are permitting to do so. As previously noted in the *Second Further Notice,* we find that this approach is appropriate because the sharing agency is in a strong position, particularly in comparison to the Commission, to make this determination based on its ''on the ground'' knowledge of the public safety-related activities, and trustworthiness, of the downstream entities with which it elects to share, *e.g.,* based on its prior interactions with such agencies.

117. We reject ATIS's view that we should ''not leave it entirely in the hands of state agencies to determine whether a local agency has a 'need to know' '' as ATIS believes this could result in misuse or unauthorized access to the information. ATIS suggests a scheme where agencies with direct access to NORS and DIRS would inform the Commission of whom they may plan to share information with in advance of a public safety event and we would then use this information to seek input from filers, including objections, prior to any information sharing. We find that the public safety benefits of our adopted approach outweigh ATIS's concerns of misuse or improper access to NORS and DIRS information. Our adopted approach ensures that decisions on how to best resolve public safety problems are in the hands of those closest to the issues (*i.e.,* participating agencies). Requiring the Commission receive notifications and solicit comments from filers, as ATIS favors, creates delays in decision making that would make NORS and DIRS information significantly less useful to participating agencies in the context of exigencies. We instead agree with Colorado Public Utilities Commission that participating agencies can make this decision more effectively and quickly given their familiarity with on the ground facts. Moreover, we find that the many safeguards that we have imposed on downstream sharing today to be directly responsive to ATIS's concerns as we believe they are sufficient to protect these sensitive

filings from misuse and unauthorized access.

118. We also reject ATIS's view that we should require that participating agencies make advance arrangements with agencies they choose to share downstream with (and that the Commission be notified of the existence of these arrangements) prior to dealing with an on-going public safety event. We are instead persuaded by the International Association of Chiefs of Police's remark that these requirements would present a ''barrier to access'' as they would consume additional resources that agencies often do not have. We decline to require that a participating agency make advance arrangements, or share at all, with other entities in light of the burden concerns expressed in the record. We find, however, that advance arrangements would likely reduce long term burdens on all parties. We therefore encourage, but do not require, participating agencies to make advance arrangements where they deem it practical and in the interests of public safety to do so.

119. We reject the views of the International Association of Chiefs of Police that we go further and require that participating agencies share information with local police agencies having a ''need to know.'' While we share the view that police agencies play a vital role in resolving many public safety issues, we decline to require participating agencies share confidential NORS and DIRS information with police agencies or any other local entity. We find that requiring Federal, state, territory, and Tribal Nation agencies to share information with other entities is incompatible with our decision today to hold the participating agency accountable for the way information is used by those entities. To maintain the reasonableness of this accountability measure, we find it critical that participating agencies be able to evaluate and select the entities (if any) with which they share information. As a practical matter, however, we expect that participating agencies will, in many cases, voluntarily share information with police agencies when a ''need to know'' exists.

120. We also reject the views of NCTA and other commenters that a participating agency should not be allowed to share directly with others outside the agency on grounds that this would risk over-disclosure. As noted above, we place safeguards on such direct sharing that will minimize the risk of unauthorized disclosure, which we find strikes an appropriate balance between disseminating NORS and DIRS information to those who can act on it, thereby savings lives and property, and protecting the sensitive nature of these filings. We also reject ACA Connects' view that the ''need to know'' of a recipient must be determined in advance of any sharing event (as opposed to in real-time during the event). We find that this provision would likely create significant and impractical delays in the transfer of critical information to non-participating agencies, particularly during times of severe exigency, and we find that the many safeguards that we've introduced on direct sharing today appropriately balance disseminating NORS and DIRS information with protecting the sensitive nature of these filings.

121. In the *Second Further Notice,* the Commission proposed to allow individuals granted credentials for direct access to NORS and DIRS filings to share copies of particular filings, in whole or part, and any confidential information derived from the filings outside their agency on a strict ''need to know' '' basis. We adopt this proposal and clarify that not only must there be a ''need to know'' for downstream sharing, but that need must pertain to a specific imminent or on-going public safety event.

122. Many state, local and industry commenters support allowing credentialed individuals at a participating agency to directly share confidential NORS and DIRS information with others outside their agency, including individuals working for local entities, on a ''need to know'' basis. We agree with Verizon and the City of New York that, while state agencies are a good initial dissemination point, effectively addressing public safety requires collaboration between state agencies and local entities (among others). We also agree with the Public Service Commission of the District of Columbia that this proposal will ''assist in developing a coordinated response to a disaster or other major outage,'' and with the Pennsylvania Public Utility Commission, which supports this proposal as necessary to ensure that information can be disseminated from participating agencies to county emergency agencies, as they are often ''the key decision-makers and first responders'' who need this information given their ''vital role . . . in ensuring public safety during times of crisis.'' We find that the proposed approach would provide a targeted and efficient way to put relevant information in the hands of local entities while minimizing the risk of over disclosure of confidential NORS and DIRS information. We also find that the proposed approach would be an effective way to ensure that PSAPs and 911 authorities that do not qualify as participating agencies can obtain relevant NORS and DIRS information.

123. We clarify, however, that not only must there be a ''need to know'' for downstream sharing, but that it must pertain to a specific imminent or on-going public safety event. Thus, in contrast with today's restrictions on sharing within a participating agency, we exclude a participating agency from sharing confidential information downstream when a potential recipient is seeking to use the information to identify trends and perform analyses related to long-term improvements in public safety outcomes. Many commenters express concerns that downstream sharing raises additional risks and would thus appear to support today's decision to further restrict the conditions on which it is permitted. We agree with commenters there is generally less accountability and an increased risk of over-disclosure when NORS and DIRS information is shared outside of those participating agencies that have been granted direct access. We similarly agree with ATIS and T-Mobile that the risks of improper use are heightened since outside recipients are not directly accountable to the Commission through our Certification Form (Appendix C). We find that these observations justify our further restriction on a ''need to know'' in the context of downstream sharing. Moreover, without this restriction in place, a participating agency could simply share all (or vast amounts) of NORS and DIRS filings with a non-participating agency on grounds of a general ''need to know,'' which would frustrate our decision to limit direct access to the many filings housed in our NORS and DIRS databases to participating agencies only.

124. *Responsibilities of Non-Participating Agencies.* The Commission proposed in the *Second Further Notice* to require that non-participating agencies that seek NORS and DIRS information first provide certification, to the supplying participating agency, that they will treat the information as confidential, not publicly disclose it absent a finding by the Commission that allows them to do so, and securely destroy the information when the public safety event that warrants its access to the information has concluded. We adopt this proposal while also requiring that non-participating agencies certify that they have completed security training using participating agencies' training materials before being granted access to NORS and DIRS filings and clarifying the meaning of ''secure'' destruction.

125. Some commenters, including state utility commissions that would incur much of the burden associated with these proposals, agree with the Commission's approach and find it workable. We agree with the Pennsylvania Public Utility Commission that requiring a non-participating agency's agreement to treat filings as confidential will help maintain NORS and DIRS filers' trust in the confidentiality of submitted information and ensure the continued success of our NORS and especially voluntary DIRS programs. We also agree with both the Colorado Public Utilities Commission and NASNA that each of these requirements is workable and can be implemented in practice even if they do impose some burden.

126. Moreover, while no commenter questioned what ''secure'' destruction would entail, we find that clarifying this term will simplify implementation of this program for non-participating agencies that are required to securely destroy information according to its terms. We clarify that the secure destruction of confidential NORS and DIRS information requires, at a minimum, securely cross-cut shredding, or machine-disintegrating, paper copies of the information, and irrevocably clearing and purging digital copies, when the public safety event that warrants access to the information has concluded.

127. We reject the Colorado Public Utilities Commission's view that a non-participating agency has a need to keep ''descriptions'' related to NORS and DIRS information in their possession to the extent it would violate our requirement for the secure destruction of the confidential NORS and DIRS information after the conclusion of a public safety event. We agree with Telecommunications Regulatory Bureau of Puerto Rico's representation from its own practice, that such reports can (and should) be ''general in nature'' and not reflect confidential NORS and DIRS information. We find that to allow a non-participating agency to keep more granular information on file is outweighed by the need to restrict the dissemination of sensitive NORS and DIRS information.

128. As noted above, we will require downstream agencies to certify that they have completed security training using participating agencies' training materials before being granted access to NORS and DIRS filings. We find that providing downstream access without any safeguards could amplify the possibility of unauthorized disclosure, particularly because downstream entities will have less experience with protecting NORS and DIRS data than participating agencies.

129. *Further downstream sharing.* In the *Second Further Notice,* the Commission proposed that the sharing of confidential NORS and DIRS information be allowed further downstream as well. According to this proposal, once an agency with direct NORS and DIRS access shared confidential NORS and DIRS information with a recipient, that recipient could further summarize and/or share the information with others that also had a ''need to know.'' Based on the record before us, we decline to adopt this proposal.

130. We find that the further downstream sharing proposal implicates several legitimate concerns around the ability to safeguard the confidentiality of the information and foster accountability among individuals and entities that would receive information. We agree with ACA Connects that the proposed approach would have made it hard to control the flow of information and maintain accountability when improper disclosure occurred. We agree with ATIS and T-Mobile that the risks of improper use would be heightened if sharing were extended to those further downstream, *i.e.,* to those not closely associated with agencies subject to our accountability measures, including as signatories to our Certification Form (Appendix C). Moreover, while some commenters suggest that these issues could be addressed through the imposition of additional safeguards, such as instituting a Commission ''coordinator'' (who would be responsible for releasing the information that is to be shared downstream and ensuring that recipients indeed have a ''need to know'') and allowing public comment on a proposed disclosure-by-disclosure basis. We reject these views as we find the proposed additional safeguards to be highly burdensome since, by adding delay to decision making, they would significantly diminish the value of the associated NORS and DIRS information in the context of exigencies.

131. We reject the views of some local entities that believe that the further downstream sharing proposal would be workable as-is. We reject these views in the context of further downstream sharing. As noted by the industry commenters, the Commission's further downstream sharing proposal would require responsible practices not just by participating agencies and those that are one ''hop'' removed from these agencies, but from a larger set of entities potentially many hops removed from the participating agency and generally not approved or cleared by the participating agency (or the Commission) in advance. We find that these public safety risks heighten, as do the difficulties of identifying the source of impermissible disclosure as information continues to be shared downstream with additional parties. Even if each individual entity taken alone has strong incentives to protect NORS and DIRS information, as Boulder Regional Emergency Telephone Service Authority contends, the risk of improper disclosure increases as a larger number of entities gains access to the information. To minimize that risk at the launch of today's new information sharing framework, we find that it is prudent to allow participating agencies to share NORS and DIRS confidential information under the conditions established in this order but not to allow further downstream sharing.

132. *Penalties and Remedies.* The Commission proposed in the *Second Further Notice* to hold participating agencies responsible for inappropriate disclosures of NORS and DIRS information by the non-participating agencies with which they share it and noted that consequences for improper disclosures by a participating agency or non-participating agency (with which the participating agency shares information) could result in termination of access to NORS and DIRS data for the participating agency. We adopt this proposal. We find that the risk of losing access is a necessary safeguard that will incentivize participating agencies to make judicious selections up-front on with whom they share NORS and DIRS information, if anyone.

133. In doing so, we reject the views of some commenters that believe that it would be unfair and a disservice to terminate a participating agency's access to NORS and DIRS information because of the potential bad actions of a non-participating entity which it cannot directly control. To further address the concerns in the record, however, we confirm that in any decision to terminate access, and set a length of time that the termination is effective, the Commission will consider the totality of the circumstances, including the reasonableness of the participating entity's decision to share information with a non-participating agency, the severity of the misuse of shared information, and the implementation of other appropriate safeguards by the implicated participating agency.

134. To address concerns of record, to the extent that a participating agency is unclear on whether specific downstream individuals or entities have a ''need to know,'' despite the clarity we

have provided on the scope of the term in today's Order, we encourage (but do not require) the agency to contact the Commission at *NORS_DIRS_information_sharing@fcc.gov* to discuss its potential sharing with the individuals and entities well in advance of a relevant public safety event.

135. We reject NASNA's suggestion that when a participating agency's direct access is terminated by the Commission, it be terminated for exactly three years, as we find this to be an unnecessarily rigid approach. We agree with Colorado Public Utilities Commission and Montrose Emergency Telephone Service Authority that a decision to terminate access need not be permanent.

136. We encourage participating agencies to proactively monitor and terminate access to non-participating agencies when they find such action warranted, but we reject Colorado Public Utilities Commission's view that the Commission should defer to participating agencies on termination decisions. The Commission has a strong incentive to safeguard all NORS and DIRS information that it receives to ensure that providers provide detailed reports on a nationwide basis.

137. The Commission will provide its remediation decisions, including its reasoning and actions to be taken to hold the participating agency accountable in a letter to the agency's coordinator, which may also be released on the Commission's website. If the Commission terminates an agency's access, the Commission will specify in the letter the time duration of this penalty as well as any conditions that must be met prior to reinstatement of access.

G. Procedures for Requesting Direct Access to NORS and DIRS

138. In the *Second Further Notice,* the Commission proposed requiring eligible state, Tribal Nation and Federal agencies to apply for direct access to NORS and DIRS filings by sending a request to the Commission's designated email address and completing a Certification Form. The request would include: (i) A signed statement from an agency official, on the agency's official letterhead, including the official's full contact information and formally requesting access to NORS and DIRS filings; (ii) a description of why the agency has a need to access NORS and DIRS filings and how it intends to use the information in practice; (iii) if applicable, a request to exceed the proposed presumptive limits on the number of individuals (*i.e.,* user accounts) permitted to access NORS and DIRS filings with an explanation of why this is necessary and (iv) a completed copy of a Certification Form, a template of which is provided in this item as Appendix C.'' On receipt, the Commission would review the request, follow-up with the agency official with any potential questions or issues. Once the Commission has reviewed the application and confirmed the application requirements are satisfied, the Commission would grant NORS and DIRS access to the agency by issuing the agency NORS and DIRS user accounts. We adopt these application procedures today, subject to the modification we have discussed above to require applying agencies to identify legal authority that charges them with promoting the protection of life or property. We find that, generally, commenters opining on the proposed procedures for requesting NORS and DIRS access raise no concerns with them. For example, the Competitive Carriers Association opines that the ''FNPRM's proposed procedures for requesting data would help to ensure data is accessed on a limited, as-needed basis.'' NASNA notes the *Second Further Notice's* proposed ''procedure for potential participating agencies to apply for direct access to NORS and DIRS data,'' and states that it ''has no objections to the procedure outlined.''

139. Other commenters urge additional modifications to the proposed procedures, which we reject. For example, ACA Connects urges the Commission ''to require agencies as part of their application to explain precisely the public safety need that justifies access to NORS or DIRS data, and to grant such access only to that extent necessary to meet that need,'' and also argues that ''a participating agency should be required to submit to the Commission the names of all individuals with whom it will share the data, along with an explanation why each individual ''needs to know'' the information.'' We decline to adopt this proposal as we expect our application requirement that legal authority be identified and certified to by agencies will address the issue of public safety need and find that requiring agencies to submit the names of all individuals with whom it will share data is inflexible and disregards that agencies might not know the full extent of individuals it will provide access to at the time of application. Furthermore, we note that Verizon suggests that applications ''could include point of contact information for localities seeking access to information in the reports.'' We also reject this recommendation as our application process is focused on reviewing the eligibility of agencies under the sharing framework and ensuring that they will adhere to the framework's safeguards and we defer to participating agencies to determine whether and how they want to establish a point of contact for requests by local agencies.

140. Moreover, some commenters propose that the Commission notify service providers when a particular agency applies for access to allow the provider to raise any concerns. For example, Verizon argues that ''if service providers have concern for the confidentiality protections available in a particular state or have other issues appropriate for the Commission's consideration, such notification would give the service provider an opportunity to raise those concerns.'' We find that, if implemented, this approach could lead to protracted disputes between service providers and participating agencies and impede efficient access to NORS and DIRS information. While Verizon does not indicate what ''other issues'' could be raised for the Commission's consideration through a notification process in its comments, the Commission expects that its objective application process and its safeguards for protecting the confidentiality of NORS and DIRS data will help prevent improper use and disclosure.

141. Furthermore, we find that eligible agencies, which have public safety duties, are unlikely to release sensitive information in ways that undermine national security or other public safety purposes. These agencies are also not in competition with service providers, and thus lack anticompetitive motives to use the information improperly. Moreover, we find that potentially contesting an agency's eligibility under our framework could detract from service provider and public safety resources that should be more immediately directed to using NORS and DIRS information to improve public safety. However, we encourage service providers to inform the Commission about any laws that would prevent any eligible agencies in a jurisdiction from maintaining the confidentiality of NORS and DIRS information, as well as any specific concerns regarding participating agencies that may be improperly accessing, using, or disclosing NORS and DIRS information.

142. Although we will not notify providers when an agency requests access to NORS and DIRS information for the aforementioned reasons, we find that providers should be kept apprised of the entities granted direct access to NORS and DIRS filings to track the use of network outage data. Therefore, we

will develop a general list of participating agencies granted access to filings under our information sharing framework that will made available to relevant service providers. This list will be updated on a periodic basis. We delegate authority to PSHSB to develop, update, and make available this list.

143. *Certification Form.* In the *Second Further Notice,* the Commission proposed the adoption of a Certification Form ''to address the certifications and acknowledgments required for direct access to NORS and DIRS filings,'' and sought comment on the various elements and requirements of the Certification Form. Based on our review of the record, we adopt the proposed Certification Form today, with slight modifications we discuss below, as we expect that it will provide for adequate acknowledgment of the confidential nature of the NORS and DIRS filings and help protect against the unauthorized use of NORS and DIRS information. We note that several commenters support the proposed Certification Form.

144. Many commenters offer various proposals for modifications intended to strengthen the safeguarding of NORS and DIRS information by requiring notice of data breaches to the Commission and service providers. We agree with commenters that it will further public safety to require participating agencies to certify that they will immediately notify the Commission and affected service providers of data breaches or the unauthorized or improper disclosure of NORS/DIRS data. CenturyLink also comments that ''State and local agencies should be required to immediately report to the service provider and the FCC any unauthorized or improper disclosure of NORS/DIRS data.'' ACA Connects further states that ''the Commission should require participating agencies to notify the Commission and affected communications providers in the event of a data breach, and should set forth appropriate penalties, including revocation of the agreement, for an agency that fails to protect or misuses the data,'' and that [a]t minimum, an agency that demonstrates a pattern of misuse or improper disclosure of NORS or DIRS data should be cut off from any further access.'' We find that in addition to enabling service providers to minimize the negative effects of improper disclosure, this modification to the Certification Form would allow the Commission to quickly identify misuse of NORS and DIRS information, further investigate violations of information sharing rules, and, if necessary, restrict continued access by offending participating agencies. NCTA also argues that ''as AT&T has previously suggested, after any improper access to or use of NORS or DIRS data by an employee, the Qualifying Governmental Agency should agree ''to perform an investigation of that employee and report the results of its investigation to the Commission and, possibly, to law enforcement.'' As we expect that the approach we adopt today will enable the Commission to coordinate the swift investigation of potentially improper uses of NORS and DIRS data, which could include investigation of personnel at participating agencies, we decline to adopt this proposal.

145. Other commenters make additional Certification Form proposals intended to ensure confidentiality and the proper use of NORS and DIRS filings, which we reject. We decline to adopt NCTA's recommendation that the Commission require participating agencies ''to certify that NORS and DIRS filings will not be accessed by individuals who are not designated employees,'' or are no longer employed by the agency. We note that non-participating agencies that receive NORS and DIRS information from participating agencies will be required to complete a certification that they will treat the information as confidential. We also expect that the training and safeguard requirements we adopt today will be sufficient to prevent unauthorized access to filings. We further find that the addition of this provision could be confusing as we note that pursuant to the rules we adopt today, participating agencies can share copies of NORS and DIRS filings, within or outside their participating agency. NCTA also recommends that a participating agency certify that, among other things, it will only use NORS and DIRS information for public safety responsibilities. ATIS also urges that the Certification Form be modified to ''specifically require agencies to certify that they have ''need to know'' this information and that they agree to use this information only for public safety purposes.'' CenturyLink also agrees with NCTA that ''a certifying agency should also describe ''how it intends to use the information in practice.'' We further find that the limitations on NORS and DIRS data described in the Certification Form—which requires agencies to certify that they will comply with the restrictions we adopt today—and our application procedures—including procedures that require agencies to identify the legal authority that charges them with public safety responsibilities—as adopted adequately address the remaining issues referenced in NCTA and other commenter's proposals.

146. In addition to these arguments, some commenters urge the Commission to adopt a certification process similar to the process the Commission has implemented to grant state access to North American Numbering Plan data, require state agencies to certify that they have adequate confidentiality protections in place, or describe the safeguards they have implemented to protect NORS and DIRS data. We reject all proposals regarding these issues to the extent that they differ from the provisions in the Certification Form we adopt today. We note that the proposed Certification Form was modeled after the certification that we require for access to North American Numbering Plan data, but enhanced to protect NORS and DIRS information, which if mishandled, implicates national security and competitive sensitivity concerns. For example, the Certification Form requires agencies to certify and acknowledge that NORS and DIRS filings are sensitive and presumed confidential for national security and commercial competitiveness reasons and report any suspected breaches to the Commission immediately.

147. In addition, we will require agencies to certify that they have implemented practical data protection safeguards including assigning user accounts to single employees, promptly reassigning user accounts to reflect changes as their rosters of designated employees change, and periodically changing user account passwords to ensure that user account credentials are not used by individuals who are not the agency's designated employees. Furthermore, the requirements we adopt today will obligate participating agencies to implement effective confidentiality safeguards regardless of the level of safeguards that exist in their states. For example, we require all participating agencies to certify that they will ''treat NORS and DIRS filings and information in accordance with procedural and substantive protections that are equivalent to or greater than those afforded under Federal confidentiality statutes and rules, including but not limited to the Federal Freedom of Information Act,'' and to ''the extent that Federal confidentiality statutes and rules impose a higher standard of confidentiality than applicable state law or regulations provide,'' the agencies must certify that they will ''adhere to the higher Federal standard.''

148. Commenters also make proposals intended to ensure the Certification Form clarifies the limitations of NORS and DIRS filings and the scope of entities eligible to receive them. For example, Verizon proposes that the Certification Form state that the recipient of filings ''further acknowledges that information reported in DIRS and NORS filings is subject to revision and correction by the reporting service provider.'' However, we find that the proposed Certification Form accounts for potential errors and inaccuracies in NORS and DIRS filings by requiring participating agencies to ''acknowledge that the Commission does not guarantee the accuracy of either the NORS or DIRS filings.'' We note that providers can share revised and corrected filings with us, which we will in turn make available to participating agencies granted access to the framework. Additionally, ATIS proposes that the Certification Form be modified to ''avoid confusion by clarifying in the opening paragraph that state agencies may get access only to reports for that state and cannot request nationwide filings.'' ATIS states that ''one way to achieve this would be replace the bracketed language with ''[for state agencies, name of states; for Federal agencies, name of states or nationwide].'' '' We agree with ATIS that we should revise the Certification Form to clarify the scope of entities that we intend to provide with access to our framework. Therefore, we add bracketed language to the Certification Form to indicate that states, the District of Columbia, Tribal Nations, and U.S. territories may be granted access only for reports of outages connected to their jurisdictions consistent with our rules.

149. We note that in addition to the Certification Form revisions we describe above, and consistent with the requirements we adopt today, we add an additional provision to the form to require the designated agency contact for each participating agency to serve as the coordinating point of contact for the agency consistent with the requirements we have described.

150. Finally, in the *Second Further Notice,* the Commission proposed to ''direct PSHSB to promulgate any additional procedural requirements that may be necessary to implement the Commission's proposals for the sharing of NORS and DIRS information, consistent with the Administrative Procedure Act.'' The Commission also stated that ''we foresee that such procedural requirements may include implementation of agency application processing procedures, necessary technical modifications to the NORS and DIRS databases (including, potentially, modifications designed to improve data protection and guard against unauthorized disclosure), and reporting guidelines to ensure that the Commission receives the notifications identified in Appendix C.'' The Commission sought comment on these proposals, and asked whether there were additional safeguards it should adopt for the application process or any other procedural requirements that would be necessary to implement the Commission's proposals. No commenters addressed these proposals or provided any evidence to rebut their necessity. Thus, we adopt them and we are confident that PSHSB's technical and administrative expertise will help facilitate the efficient implementation of the information sharing framework to further enhance public safety as contemplated by the rules we adopt today.

H. Effective Dates

151. In the *Second Further Notice,* the Commission proposed to have the Public Safety and Homeland Security Bureau issue a Public Notice that would (a) announce OMB approval of any new information collection requirements that the Commission might adopt in modifying the DIRS and NORS regime; and (b) set a date on which (i) service providers would be required to conform any new filings in NORS and DIRS to any newly adopted reporting protocols; and (ii) agencies could file certification forms requesting access to those reports. Thus, direct NORS and DIRS access would become available to eligible agencies as of the specified date. Moreover, the Commission proposed that the date set by the Bureau would be a date after the technical adjustments necessary to facilitate sharing had been made to the Commission's NORS and DIRS databases. The Commission tentatively concluded in the *Second Further Notice* that adoption of this proposal would give interested agencies ample time to prepare their certifications and give service providers sufficient time to adjust their NORS and DIRS filing processes to conform with technical changes required by today's final rule changes. While no commenter opposed our proposals, we find it in the public interest to adopt the proposals with one modification, *i.e.,* to specify an effective date, subject to extension, as part of today's decision.

152. We find that this approach provides the Commission adequate time to implement the regime contemplated by today's rules and will permit the Bureau time to account for contingencies, *i.e.,* the readiness of the databases and the OMB approval that facilitates the implementation of the revised regime. Our experience in other contexts informs our estimate that the NORS and DIRS database adjustments and related transition to implement the new requirements will require approximately 18 months. Accordingly, we set an effective date below of September 30, 2022 for the revisions to section 4.2. We delegate authority to the Public Safety and Homeland Security Bureau, which will seek OMB review and make adjustments to the databases, to extend this effective date if necessary by Public Notice published in the **Federal Register** (*e.g.,* if database adjustments take longer than we estimate here or if the required OMB review of the modified information collections under the new rule provisions is delayed).

IV. Procedural Matters

153. *Final Regulatory Flexibility Analysis.* The Regulatory Flexibility Act of 1980, as amended (RFA), requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that ''the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.'' Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this *Second Report and Order* on small entities. The FRFA is set forth in Appendix B.

154. *Paperwork Reduction Act Analysis.* As described at paras. 83 and 84, *supra,* service providers will be required to make adjustments to their NORS reporting processes, to accommodate the Commission's adjustments to its NORS web-based form, pursuant to section 47 CFR 4.11 of the Commission rules. These adjustments and today's new requirement that agencies file certification forms, pursuant to section 4.2, to request access to NORS and DIRS reports, constitute a modified information collection. They require that service providers modify their NORS reporting processes to provide the Commission with jurisdiction-specific reports and that participating agencies begin to provide the Commission with certification forms and reports and information related to known or reasonably suspected unauthorized use or improper disclosure of confidential NORS and DIRS information. These modified information collections will be submitted to the Office of Management and Budget (OMB) for review under

section 3507(d) of the Paperwork Reduction Act of 1995 (PRA). OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. This document will be submitted to OMB for review under section 3507(d) of the PRA. In addition, we note that, pursuant to the Small Business Paperwork Relief Act of 2002, the Commission previously sought, but did not receive, specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. The Commission does not believe that the new or modified information collection requirements will be unduly burdensome on small businesses. Applying these new or modified information collections will promote public safety response efforts, to the benefit of all size governmental jurisdictions, businesses, equipment manufacturers, and business associations by providing better situational information related to the nation's network outages and infrastructure status. We describe impacts that might affect small businesses, which includes most businesses with fewer than 25 employees, in the FRFA in Appendix B.

155. *Further Information.* For further information, contact Saswat Misra, Attorney-Advisor, Cybersecurity & Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418–0944 or via email at *Saswat.Misra@fcc.gov.*

V. Ordering Clauses

156. *Accordingly it is ordered* that, pursuant to the authority contained in sections 1, 4(i), 4(j), 4(o), 251(e)(3), 254, 301, 303(b), 303(g), 303(r), 307, 309(a), 309(j), 316, 332, and 403, of the Communications Act of 1934, as amended, and section 706 of the Telecommunications Act of 1996, 47 U.S.C. 151, 154(i)–(j) & (o), 251(e)(3), 254, 301, 303(b), 303(g), 303(r), 332, 403, and 1302, this Second Report and Order in PS Docket No. 15–80 is *adopted.*

157. *It is further ordered* that the amendments of the Commission's rules as set forth in Appendix A *are adopted*, effective September 30, 2022, as described at § III.H, above.

158. The Commission will submit this *Second Report and Order* to the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, for concurrence as to whether these rules are ''major'' or ''non-major'' under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of this *Second Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

Final Regulatory Flexibility Analysis

159. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications, Second Further Notice of Proposed Rulemaking (Second Further Notice).* The Commission sought written public comment on the proposals in the *Second Further Notice,* including comment on the IRFA. No comments were received specifically addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.

A. Need for, and Objectives of, the Second Report and Order

160. In the *Second Report and Order,* the Commission adopts various proposals made in the *Second Further Notice* adopted in February 2020. We take specific steps to share the Commission's network outage and infrastructure status information with state and Federal Government agencies and others whose official duties make them directly responsible for emergency management and first responder support functions (*i.e.,* have a ''need to know'').

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

161. No comments were submitted specifically in response to the IRFA, however a few commenters expressed concerns about the estimated costs to service providers discussed by the Commission in the *Second Further Notice.* Despite these concerns however, none of the commenters provided any cost data or analysis to support their concerns or rebut the Commission's cost estimates in accordance with the Commission's request for such data in the *Second Further Notice.* Similarly, while some state agency and advocacy organizations expressed concerns that it will be burdensome for voluntarily participating agencies to relay information they retrieve from the NORS and DIRS databases to other permissible ''downstream'' entities as allowed by the adopted information sharing framework, none of these entities attempt to quantify the costs associated with these activities.

162. Moreover, the Commission is unaware of any alternative approaches with lower costs, nor have any been identified by commenters, that would still ensure that the Commission promptly and reliably learns of the actions described above that may lead to the disclosure of NORS or DIRS-related information. Lessening the promptness or reliability of notifications to the Commission would disincentivize providers from supplying robust and fulsome NORS and DIRS reports and therefore reduce the benefits that those filings would provide to the Commission and participating agencies alike. We find that this reduction in benefits would outweigh the expected modest cost savings to those participating agencies that would be required to provide notifications under the framework we adopt today.

C. Response to Comments by Chief Counsel for Advocacy of the Small Business Administration

163. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments. No comments were filed by the SBA.

D. Description and Estimate of the Number of Small Entities to Which Rules Will Apply

164. The RFA directs agencies to provide a description of, and, where feasible, an estimate of, the number of small entities that may be affected by the rules adopted herein. The RFA generally defines the term ''small entity'' the same as the terms ''small business,'' ''small organization,'' and ''small governmental jurisdiction.'' In addition, the term ''small business'' has the same meaning as the term ''small business concern'' under the Small Business Act. A small business concern is one which: (1) Is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA). Such entities include Interconnected VoIP services, Wireline Providers, Wireless Providers—Fixed and Mobile, Satellite Service Providers, and Cable Service Providers.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

165. *Service Providers.* The rules adopted in the *Second Report and Order* require service providers to make minor adjustments to their existing reporting process to account for new or refined multistate reporting for the NORS filings.

166. *Voluntarily participating agencies.* Pursuant to the confidential protections adopted in the *Second Report and Order,* voluntarily participating agencies, including those that are small entities, will be required to notify the Commission when they receive requests for NORS filings, DIRS filings, or related records, and prior to the effective date of any change in relevant statutes of laws that would affect the agency's ability to adhere to the confidentiality protections that the Commission requires. Under the adopted information sharing framework, voluntarily participating agencies will also be required to submit to the Commission requests for direct access to NORS and DIRS filings which include a description of why the agency has a need to access NORS and DIRS filings (''need to know'') and how it intends to use the information in practice. Agencies applying for direct access to NORS and DIRS are required to demonstrate their ''need to know'' by citing to legal authority, in the form of a statutes, rules, court decisions, or other binding legal provisions, establishing that it has official duties involving preparing for, or responding to, an event that threatens public safety.

167. Additionally, participating agencies will be required to implement initial and annual security training to each person granted a user account for NORS and DIRS filings, and certify that they will take appropriate steps to safeguard the information contained in the filings, including notifying the Commission of unauthorized or improper disclosure. In the event of any known or reasonably suspected breach of protocol involving NORS and DIRS filings participating agencies will be required to report this information to the Commission and all affected providers immediately. Participating agencies will also be required to maintain and make available for inspection, upon Commission request, a list of all localities for which the agency has disclosed NORS and DIRS data.

168. In the *Second Report and Order,* the Commission allows participating agencies to share confidential NORS and DIRS information within an outside the agency subject to certain limitations. Participating agencies will also be required to execute an annual attestation form certifying and acknowledging compliance with requirements of the information sharing framework that the Commission adopts.

F. Steps Taken To Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

169. The Commission has taken specific steps minimize costs for both service providers and voluntarily participating agencies in the NORS and DIRS information sharing framework adopted in the *Second Report and Order.* The Commission did not make DIRS reporting mandatory as urged by some commenters in the proceeding. Moreover, while the Commission adopted changes to the NORS form filing to allow users to select more than one state when submitting a request for NORS information that modified the method in which service providers report outage information in NORS, this change did not impose additional levels of reporting to require disaggregation to provide a breakout of state-specific impacts by submitting state specific filings We note that service providers will not need to modify their DIRS reporting processing to accommodate multistate reporting. To provide participating agencies maximum flexibility and reduce potential costs of compliance with the training requirements, rather than mandate an agency's use of a specific training program, we adopted requirements that allow agencies to develop their own training program or rely on an outside training program that covers, at a minimum, a set of five ''program elements.''

170. In addition, rather than requiring third-party audits of training programs to ensure that state and Federal agencies' training programs comply with the Commission's proposed required program elements, participating agencies are required to make copies of their training curriculum available for the Commission's review upon demand which will significantly minimize costs associated with the required training programs. The Commission also declined to adopt a ''downstream training'' requirement which would have required any entity receiving NORS & DIRS information from a participating agency to complete formal training. Similarly, the Commission declined to adopt a requirement for participating agencies to obtain an affidavit on confidentiality from local entities prior to receipt NORS and DIRS information. To further assist and reduce the burden on small entities and other participating agencies with meeting the training requirements the Commission adopted in the *Second Report and Order,* the Commission will consult with diverse stakeholders with a range of perspectives, including state governments, the public safety community, service providers, and other industry representatives to develop exemplar training materials, that can be used by participating agencies to training their staffs on the proper uses of NORS and DORS filings.

171. The Commission also declined to grant local agencies direct access to NORS and DIRS considering among other things the burdens that would result for local entities, many of which may be small entities. Additionally, the Commission has adopted a single form to address the certifications and acknowledgments required for direct access to NORS and DIRS. The use of a single form, coupled with the fact that the proposed certification form is similar to one that the Commission currently requires for sharing sensitive numbering data with states using FCC Form 477 data, should help minimize preparation time and costs, specifically for those smaller agencies since these agencies should be familiar with the existing requirements and have comparable operational processes and procedures already in place.

Certification Form

Instructions: Please review and complete the form below. Please send your completed form to *NORS_DIRS_information_sharing@fcc.gov.* On review, the Commission will contact you to resolve any questions with your application papers or issue your agency login credentials for accessing NORS and DIRS.

[NAME OF AGENCY]

CERTIFICATION FORM FOR NORS AND DIRS SHARING

[your title]
[name of agency]
[address]
[address]

Dear Commission:

[Agency name] requests access to Network Outage Reporting System (NORS) and Disaster Information Reporting System (DIRS) filings involving [for states, the District of Columbia, or U.S. Territories, the name of state(s) or jurisdiction(s); for Federal agencies, the name of state(s) or nationwide; for Tribal nations, the name of the Tribal Government or component thereof] (filings).

I hereby certify and acknowledge that I am authorized to act on behalf of the [name of agency] and that [name of agency] is willing and able to be bound by the terms and conditions provided in this document.

On behalf of [agency name], I acknowledge and certify that [agency name] agrees to the terms below.

I hereby certify and acknowledge that each user account is to be assigned to a single employee and that [agency name] will promptly reassign user accounts to reflect changes as its roster of designated employees changes (*e.g.,* due to employee departure and arrival).

I hereby certify and acknowledge that [agency name] will change user account passwords and take other reasonable measures to ensure that user account credentials are not used by individuals who are not [agency name]'s designated employees.

I hereby certify and acknowledge that NORS and DIRS filings, and the information contained therein (collectively, NORS and DIRS filings and information) are sensitive and presumed confidential for national security and commercial competitiveness reasons.

I hereby certify that [agency name] will treat NORS and DIRS filings and data as confidential under Federal and state Freedom of Information Act statutes and similar laws and regulations and not disclose them absent a finding by the Commission that allows [agency name] to do so.

I hereby certify that [agency name] will treat NORS and DIRS filings and information in accordance with procedural and substantive protections that are equivalent to or greater than those afforded under Federal confidentiality statutes and rules, including but not limited to the Federal Freedom of Information Act. 5 U.S.C. 552(b)(4). To the extent that Federal confidentiality statutes and rules impose a higher standard of confidentiality than applicable state, U.S. territory, or Tribal law or regulations provide, I represent that the [name of agency] is legally able to and will adhere to the higher Federal standard. I agree that the [name of agency] will notify the Commission, within 14 calendar days via the email, *NORS_DIRS_information_sharing@fcc.gov,* when [name of agency] receives a request from a third party to disclose NORS filings and DIRS filings, or related records, pursuant to a state's open record laws or other legal authority that could compel [name of agency] to do so. I agree to notify the Commission via the email, *NORS_DIRS_information_sharing@fcc.gov,* at least 30 calendar days prior to the effective date of any change in relevant statutes of laws that would affect [name of agency]'s ability to adhere to at least the Federal confidentiality rules and statutes standard.

I hereby certify and acknowledge that the Commission's rules place restrictions on the access to and use of NORS and DIRS filings and information. I certify that I have reviewed and agree to comply with the restrictions regarding information sharing as described in part 4 of Title 47 of the Code of Federal Regulations.

I hereby certify and acknowledge that the [name of agency] will adopt or develop a NORS and DIRS security training program, if it has not already, that satisfies each of the required training program elements identified at [cite to forthcoming Order], that the [name of agency] will administer this training to each of its designated employees prior to their access to NORS and DIRS filings and information and then at least annually thereafter. The [name of agency] will make copies of its training curriculum available for the Commission's review upon demand.

I further acknowledge that [name of agency] will report immediately to any affected service providers and to the Commission, via the email *NORS_DIRS_information_sharing@fcc.gov* and *NSOC@fcc.gov*, any known or reasonably suspected breach of the protocol specified in the training program or any other known or reasonably suspected unauthorized use or improper disclosure of NORS and DIRS information.

I further acknowledge that if [name of agency] needs contact information for a provider, that [agency name] may request this information from the Commission at *NORS_DIRS_information_sharing@fcc.gov,* and that this does not toll [agency name]'s obligation to immediately notify any affected service providers, using the best contact information known to [agency name].

I acknowledge on behalf of [name of agency] that the Commission does not guarantee the accuracy of either the NORS or DIRS filings as both sets of filings are submitted to the respective web-based databases by service providers pursuant to mandatory reporting timeframes for NORS filings and voluntary reporting timeframes for DIRS filings. Further, I acknowledge that there may be times access to the filings is unavailable, *e.g.,* due to planned or unplanned service and maintenance.

I hereby certify and acknowledge that [agency name's] continued access to NORS and DIRS filings and information is conditioned on its annual recertification of a current version of this form, available on the Commission's website. I acknowledge that the Public Safety and Homeland Security Bureau (Bureau) of the Commission may terminate [agency name]'s access at any time, and for any reason, by giving written notice to [name of agency]. If access is terminated, I agree that [name of agency] will, upon the Commission's termination notice, cause to be securely destroyed any and all NORS and DIRS filings and information or other data received pursuant to this grant, whether electronic or hardcopy form.

I hereby certify and acknowledge that all the terms and conditions provided in this document apply to past and future NORS and DIRS filings and information.

I hereby certify that [employee name, title, phone number and email address] will manage my agency's access to NORS and DIRS filings by managing user accounts in accordance with the Commission's rules; coordinating the downstream sharing of NORS and DIRS filings; making available for Commission inspection a list of all localities for which the agency has disclosed NORS and DIRS data; coordinating with the Commission to manage an unauthorized access incident; and answering any questions from the Commission regarding my agency's access, use, or sharing of NORS and DIRS filings.

I hereby certify and acknowledge my and [agency name]'s obligation to inform the Commission if I cease to be the designated representative of [agency name] with authority to obligate and bind the agency to the statements above or if the employee listed above ceases to be the designated agency contact.

I acknowledge that the Bureau makes no determinations about any provisions of [name of state] law or agency regulations or your statements about such provisions.

Sincerely,

[name and title of official], on behalf of [name of agency]

Affirmed:

Lisa M. Fowlkes
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Exemplar Aggregated Data

Overview

The following provides general non-binding guidelines regarding how to aggregate NORS and DIRS data, followed by examples of aggregated NORS and DIRS data based on hypothetical information. The aggregated data presented does not reflect the exact number of users affected by a service provider's outage and is only used for situational awareness. We remind agencies participating in our framework that failure to properly aggregate data in accordance with the rules adopted in the *Second Order* could lead to the improper disclosure of service providers' confidential information and may result in termination of their access to NORS and DIRS filings by the Commission. Participating agencies with additional questions are urged to contact the Commission for guidance.

General Aggregation Guidelines

Aggregation 'Dos'

- It is best to aggregate only NORS and DIRS information of the same type (*e.g.,* aggregate wireless data and wireline data separately). If information is aggregated across different types, the public release of this information should state the types of NORS or DIRS information aggregated (*e.g.* ''This data includes wireless and wireline data'').
- It is best to aggregate 911 outages according to their impact (*e.g.,* 911 call delivery affected, only 911-caller location information affected). If information is aggregated across different types of 911 outages, the public release of this information should note the approximate proportion of the effects (*e.g.,* ''in most cases only location information is affected'').
- If aggregating NORS information, aggregate information related to long-term trends using final reports only.

• If aggregating NORS information from notifications or initial reports, please be aware that this information may change as service providers further remediate or investigate the outage. It is recommended that agencies make clear that this information is only preliminary and may change or be updated over time.

• If several reported outages seem very large, it is good practice to confirm the magnitude of the outage with the reporting service providers prior to releasing any aggregated information about them. In some instances, service providers may intentionally overestimate the effect of an outage out of an abundance of caution. Agencies should be aware of these circumstances prior to determining what information would be appropriate to release to the public.

• If an agency intends to aggregate the duration or the number of users affected by multiple outages, reporting the median is generally preferred over reporting the mean (average) because the mean may be skewed by unrepresentatively high or low outliers.

• When aggregating data for incidents occurring over a period of time, use the incident date/time, not the creation date or reportable date.

• The frequency of NORS outage reports varies by season. If aggregating for the purpose of comparing two time periods, it is advisable that the time periods be of the same season of the year (*e.g.,* compare January to March 2020, to January to March 2019, but not to July to August 2019.)

• Be careful when aggregating outages with durations of all 9's that are greater than 99 (*e.g.,* 999, 9999, 99999). These values can be indicators that the outage is ongoing even though the report is final. If in doubt, it is best to contact the reporting service provider and/or exclude these outages from the aggregation.

• Sudden increases or decreases in NORS reports may be the result of reporting rules changes or other effects. If sudden changes are noticed, the FCC should be consulted before data is made public. As a corollary, personnel responsible for data aggregation should keep up with any NORS rule changes.

Aggregation 'Don'ts'

• Do not release NORS data for a single outage, even if the name of the service provider is not mentioned in the release. Aggregation should always occur across at least four service providers, meaning that in most instances, agencies cannot release aggregated information about an ongoing outage.

• Do not aggregate data over a geographic region which has fewer than four service providers of that type in the region. For example, if a county is served by only three wireless service providers, do not report an aggregation of wireless outage data for that county.

• Do not aggregate NORS and DIRS data together.

• Do not aggregate NORS data at a scope smaller than a state, unless the reports you are aggregating all specify a smaller region (*e.g.,* a specific county or Tribal territory).

• In NORS, do not aggregate non-service affecting outages (*i.e.,* OC3 Simplex outages) with service affecting outages.

• Do not identify names of service providers as sources of outage data.

• Do not use the time zone data in NORS to determine outage location. This data is used only to identify the time zone for the incident time.

• Do not include Special Facilities outage reports in any aggregation.

Examples of Aggregated NORS and DIRS Data

NORS Example

The following table shows the total number of wireline users affected by wireline outages in each state as reported by 4 companies or more:

BILLING CODE 6712–01–P

Outage ID	Company	Reason Reportable	State Affected	Incident Date/Time	Duration Hours	Duration Minutes	Wireline Users Affected
ON-XXXX3471	Company 1	Wireline - 900,000 user-minutes	OHIO	1/4/2018 20:36	10	39	2,450
ON-XXXX3475	Company 4	Wireline - 900,000 user-minutes	OHIO	1/5/2018 20:36	4	35	43,540
ON-XXXX3477	Company 3	Wireline - 900,000 user-minutes	OHIO	1/6/2018 20:36	6	53	35,000
ON-XXXX3575	Company 4	Wireline - 900,000 user-minutes	OHIO	1/7/2018 20:36	0	30	40,313
ON-XXXX3580	Company 3	Wireline - 900,000 user-minutes	OHIO	1/8/2018 20:36	3	11	257,690
ON-XXXX3581	Company 2	Wireline - 900,000 user-minutes	OHIO	1/9/2018 20:36	5	28	23,434
ON-XXXX3582	Company 3	Wireline - 900,000 user-minutes	OHIO	1/10/2018 20:36	14	6	22,720
ON-XXXX3590	Company 3	Wireline - 900,000 user-minutes	OHIO	1/11/2018 20:36	10	7	10,897
ON-XXXX3591	Company 5	Wireline - 900,000 user-minutes	OHIO	1/12/2018 20:36	8	16	42,480
ON-XXXX3592	Company 3	Wireline - 900,000 user-minutes	OHIO	1/13/2018 20:36	3	11	257,690
ON-XXXX3593	Company 2	Wireline - 900,000 user-minutes	OHIO	1/14/2018 20:36	5	28	23434
ON-XXXX3598	Company 2	Wireline - 900,000 user-minutes	OHIO	1/15/2018 20:36	14	6	22,720
ON-XXXX3472	Company 1	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/4/2018 20:36	10	7	10,897
ON-XXXX3474	Company 2	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/5/2018 20:36	8	16	42480
ON-XXXX3479	Company 4	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/6/2018 20:36	2	6	116000
ON-XXXX3481	Company 3	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/7/2018 20:36	26	6	1,624
ON-XXXX3560	Company 3	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/8/2018 20:36	21	35	234235
ON-XXXX3578	Company 1	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/9/2018 20:36	6	21	59,647
ON-XXXX3579	Company 2	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/10/2018 20:36	11	27	8,860
ON-XXXX3595	Company 1	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/11/2018 20:36	10	39	2450
ON-XXXX3599	Company 3	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/12/2018 20:36	4	35	43,540
ON-XXXX3600	Company 1	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/13/2018 20:36	6	53	35,000
ON-XXXX3601	Company 5	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/14/2018 20:36	0	30	40313
ON-XXXX3602	Company 1	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/15/2018 20:36	3	11	257690
ON-XXXX3603	Company 1	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/16/2018 20:36	5	28	23434
ON-XXXX3604	Company 1	Wireline - 900,000 user-minutes	PENNSYLVANIA	1/17/2018 20:36	14	6	22720
ON-XXXX3476	Company 1	Wireline - 900,000 user-minutes	VIRGINIA	1/5/2018 20:36	10	7	10,897
ON-XXXX3480	Company 2	Wireline - 900,000 user-minutes	VIRGINIA	1/6/2018 20:36	8	16	42480
ON-XXXX3482	Company 3	Wireline - 900,000 user-minutes	VIRGINIA	1/7/2018 20:36	2	6	116,000
ON-XXXX3485	Company 1	Wireline - 900,000 user-minutes	VIRGINIA	1/8/2018 20:36	26	6	1,624
ON-XXXX3487	Company 1	Wireline - 900,000 user-minutes	VIRGINIA	1/9/2018 20:36	3	11	257690
ON-XXXX3490	Company 4	Wireline - 900,000 user-minutes	VIRGINIA	1/10/2018 20:36	5	28	23434
ON-XXXX3502	Company 1	Wireline - 900,000 user-minutes	VIRGINIA	1/11/2018 20:36	14	6	22,720
ON-XXXX3507	Company 3	Wireline - 900,000 user-minutes	VIRGINIA	1/12/2018 20:36	10	7	10,897
ON-XXXX3517	Company 2	Wireline - 900,000 user-minutes	VIRGINIA	1/13/2018 20:36	8	16	42,480
ON-XXXX3530	Company 1	Wireline - 900,000 user-minutes	VIRGINIA	1/14/2018 20:36	2	6	116000
ON-XXXX3531	Company 1	Wireline - 900,000 user-minutes	VIRGINIA	1/15/2018 20:36	26	6	1624

For the NORS aggregation example table below, the number of wireline users affected from all reports above per state were added and are presented in the total number of wireline users affected per state:

State Affected	Wireline Users Affected
OHIO	782,368
PENNSYLVANIA	898,890
VIRGINIA	645,846

DIRS Example

The following table shows the total number of cell sites were affected by a disaster in each state as reported by 4 companies or more:

ID Number	Company	County	Percent of Historical Capacity Available	Cell Sites Served	Cell Sites Affected (Down)	Cell Sites Out Due to Cell Site Damage	Cell Sites Out Due to Transport	Cell Sites Out Due to No Power at Cell	Cell Sites on Back-Up Power	State	Updated
0XX-XXXXXXXX X1561	Company 1	County	99	164	1	0	1	0	0	CALIFORNIA	19:19.0
0XX-XXXXXXXX X1562	Company 2	County	100	26	0	0	0	0	0	CALIFORNIA	19:19.0
0XX-XXXXXXXX X1563	Company 3	County	99.82	1623	3	0	0	0	0	CALIFORNIA	03:53.0
0XX-XXXXXXXX X1564	Company 4	County	100	2238	4	3	1	0	0	CALIFORNIA	24:21.0
0XX-XXXXXXXX X1565	Company 1	County	100	8	0	0	0	0	0	FLORIDA	19:19.0
0XX-XXXXXXXX X1566	Company 2	County	100	23	0	0	0	0	0	FLORIDA	19:19.0
0XX-XXXXXXXX X1567	Company 3	County	100	203	0	0	0	0	0	FLORIDA	19:19.0
0XX-XXXXXXXX X1568	Company 4	County		9	3	0	1	2	0	FLORIDA	56:04.0
0XX-XXXXXXXX X1569	Company 5	County		14	5	0	2	3	0	FLORIDA	56:04.0
0XX-XXXXXXXX X1570	Company 1	County		148	26	0	10	16	0	FLORIDA	56:04.0
0XX-XXXXXXXX X1571	Company 2	County	100	50	0	0	0	0	0	FLORIDA	02:42.0
0XX-XXXXXXXX X1572	Company 3	County	100	9	0	0	0	0	0	GEORGIA	57:15.0
0XX-XXXXXXXX X1573	Company 4	County	100	2	0	0	0	0	0	GEORGIA	58:09.0
0XX-XXXXXXXX X1574	Company 5	County	100	24	0	0	0	0	0	GEORGIA	58:25.0
0XX-XXXXXXXX X1575	Company 3	County	100	33	0	0	0	0	0	GEORGIA	58:42.0
0XX-XXXXXXXX X1576	Company4	County		95	13	0	0	13	0	GEORGIA	56:04.0
0XX-XXXXXXXX X1577	Company 2	County		233	0	0	0	0	0	GEORGIA	56:04.0
0XX-XXXXXXXX X1578	Company 1	County	100	285	0	0	0	0	1	GEORGIA	03:04.0
0XX-XXXXXXXX X1579	Company 1	County		33	11	0	4	7	0	PENNSYLVANIA	56:04.0
0XX-XXXXXXXX X1580	Company 2	County		126	0	0	0	0	0	PENNSYLVANIA	04:52.0
0XX-XXXXXXXX X1581	Company 3	County		126	0	0	0	0	0	PENNSYLVANIA	05:36.0
0XX-XXXXXXXX X1582	Company 4	County	100	28	0	0	0	0	0	PENNSYLVANIA	24:28.0
0XX-XXXXXXXX X1583	Company 5	County	100	13	0	0	0	0	0	PENNSYLVANIA	24:28.0
0XX-XXXXXXXX X1584	Company 3	County	100	16	0	0	0	0	0	PENNSYLVANIA	24:28.0
0XX-XXXXXXXX X1585	Company 1	County	100	46	0	0	0	0	0	PENNSYLVANIA	24:28.0
0XX-XXXXXXXX X1586	Company 2	County	100	1	0	0	0	0	0	PENNSYLVANIA	24:28.0
0XX-XXXXXXXX X1587	Company 3	County	100	37	0	0	0	0	0	PENNSYLVANIA	58:32.0

For the DIRS aggregation example table below, the number of cell sites affected from all wireless reports above for each state were added and presented in the total number of affected cell sites per state in the table below. The percentage of cell sites out of service were calculated by dividing the number of cell sites served by the number of cell sites out of service for each state:

State Affected	Sum of Cell Sites Served	Sum of Cell Sites Out of Service	Sum of Cell Sites Out Due to Cell Site Damage	Sum of Cell Sites Out Due to Transport	Sum of Cell Sites Out Due to No Power	Percent Cell Sites Out of Service
CALIFORNIA	4051	8	3	2	0	0.20%
FLORIDA	455	34	0	13	21	7.47%
GEORGIA	681	13	0	0	13	1.91%
PENNSYLVANIA	426	11	0	4	7	2.58%

List of Subjects in 47 CFR Part 4

Airports, Communications common carriers, Communications equipment, Reporting and recordkeeping requirements, Telecommunications.

Federal Communications Commission.

Marlene Dortch,

Secretary.

Final Rule

For the reasons set forth above, part 4 of title 47 of the Code of Federal Regulations is amended as follows:

PART 4—DISRUPTIONS TO COMMUNICATIONS

■ 1. The authority citation for part 4 continues to read as follows:

Authority: 47 U.S.C. 34–39, 151, 154, 155, 157, 201, 251, 307, 316, 615a–1, 1302(a), and 1302(b); 5 U.S.C. 301, and Executive Order no. 10530.

■ 2. Section 4.2 is revised to read as follows:

§ 4.2 Availability of reports filed under this part.

Reports filed under this part will be presumed to be confidential under § 0.457(d)(1) of this chapter. Notice of any requests for inspection of outage reports will be provided pursuant to § 0.461(d)(3) of this chapter except that the Chief of the Public Safety and Homeland Security Bureau may grant, without providing such notice, an agency of the states, the District of Columbia, U.S. territories, Federal Government, or Tribal Nations direct access to portions of the information collections affecting its respective jurisdiction after the requesting agency has certified to the Commission that it has a need to know this information and has protections in place to safeguard and limit the disclosure of this information as described in the Commission's Certification Form for NORS and DIRS Sharing (Certification Form). Sharing is restricted by the following terms:

(a) Requesting Agencies granted direct access to information collections must report immediately to any affected service providers and to the Commission any known or reasonably suspected unauthorized use or improper disclosure, manage their agency's access to outage reports by managing user accounts in accordance with the Commission's rules, coordinate with the Commission to manage an unauthorized access incident, and answer any questions from the Commission regarding their agency's access, use, or sharing of reports.

(b) Agencies granted direct access to information collections may share copies of the filings, and any confidential information derived from the filings, outside their agency on a strict need-to-know basis when doing so pertains to a specific imminent or on-going public safety event. The agency must condition the recipients' receipt of confidential NORS and DIRS information on the recipients' certification, on a form separate from the Certification Form, that they will treat the information as confidential, not publicly disclose it absent a finding by the Commission that allows them to do so, and securely destroy the information by, at a minimum, securely cross-cut shredding, or machine-disintegrating, paper copies of the information, and irrevocably clearing and purging digital copies, when the public safety event that warrants access to the information has concluded.

(c) Except as permitted pursuant to paragraph (b) of this section, agencies granted direct access to information collections may not share filings, or any confidential information derived from the filings, with non-employees of the agency, including agency contractors, unless such sharing is expressly authorized in writing by the Commission.

(d) Agencies granted direct access to information collections may disseminate aggregated and anonymized information to the public. Such information must be aggregated from at least four service providers and must be sufficiently anonymized so that it is not possible to identify any service providers by name or in substance.

(e) Consequences for an Agency's failure to comply with these terms may result in, among other measures, termination of direct access to reports by the Commission for a time period to be determined by the Commission based on the totality of the circumstances surrounding the failure.

[FR Doc. 2021–07457 Filed 4–28–21; 8:45 am]

BILLING CODE 6712–01–C