



6712-01

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 4

[PS Docket No. 15-80; FCC 20-20; FRS 16584]

Disruptions to Communications

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Commission seeks comment on a proposed a framework to provide state and federal agencies with access to outage information to improve their situational awareness while preserving the confidentiality of this data, including proposals to: provide direct, read-only access to NORS and DIRS filings to qualified agencies of the 50 states, the District of Columbia, Tribal nations, territories, and federal government; allow these agencies to share NORS and DIRS information with other public safety officials that reasonably require NORS and DIRS information to prepare for and respond to disasters; allow participating agencies to publicly disclose NORS or DIRS filing information that is aggregated and anonymized across at least four service providers; condition a participating agency's direct access to NORS and DIRS filings on their agreement to treat the filings as confidential and not disclose them absent a finding by the Commission that allows them to do so; and establish an application process that would grant agencies access to NORS and DIRS after those agencies certify to certain requirements related to maintaining confidentiality of the data and the security of the databases.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**; and reply comments on or before

[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by PS Docket No. 15–80, by any of the following methods:

- *Federal Communications Commission’s Web site:* <http://fjallfoss.fcc.gov/ecfs2/>. Follow the instructions for submitting comments.
- Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. See the **SUPPLEMENTARY INFORMATION** section for more instructions.
- *People with Disabilities:* Contact the FCC to request reasonable accommodations (accessible format documents, sign language interpreters, CART, etc.) by email: FCC504@fcc.gov or phone: 202–418–0530 or TTY: 202– 418–0432.

For detailed instructions for submitting comments and additional information on the rulemaking process, see the **SUPPLEMENTARY INFORMATION** section of this document.

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 or Brenda D. Villanueva, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418–7005 or via email at Brenda.Villanueva@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission’s Second Further Notice of Proposed Rulemaking (*FNPRM*), PS Docket No. 15-80; FCC 20–20, adopted on February 28, 2020, and released on March 2, 2020. The full text of this document is available

for inspection and copying during normal business hours in the FCC Reference Center (Room CY–A257), 445 12th Street SW., Washington, DC 20554 or via ECFS at <http://fjallfoss.fcc.gov/ecfs/>. The full text may also be downloaded at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-63A1.pdf.

Pursuant to §§ 1.415 and 1.419 of the Commission’s rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission’s Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- *Electronic Filers*: Comments may be filed electronically using the Internet by accessing the ECFS: <http://apps.fcc.gov/ecfs/>.
- *Paper Filers*: Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission’s Secretary, Office of the Secretary, Federal Communications Commission.

- All hand-delivered or messenger-delivered paper filings for the Commission’s Secretary must be delivered to FCC Headquarters at 445 12th St. SW., Room TW–A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners.

Any envelopes and boxes must be disposed of before entering the building.

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street SW., Washington, DC 20554.

People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice), 202– 418–0432 (tty).

Synopsis

I. INTRODUCTION

1. The Commission supports our Nation’s incident preparedness goals and emergency response efforts by, among other things, collecting and providing accurate and timely communications outage and infrastructure status information via our Network Outage Reporting System (NORS) and Disaster Information Reporting System (DIRS). NORS and DIRS provide critical information about significant disruptions or outages to communication services, including among others, wireline, wireless, cable, broadcast (radio and television), satellite, and interconnected VoIP, as well as communications disruptions affecting Enhanced 9-1-1 facilities and airports. Given the sensitive nature of this data to both national security and commercial competitiveness, the outage data is presumed to be confidential.

2. Today when a major disaster or outage occurs, we make this information available to the Department of Homeland Security’s (DHS) National Cybersecurity and

Communications Integration Center (NCCIC). DHS uses this information to assess the needs of an affected area and to coordinate overall emergency response efforts with state and local first responders so that assets such as equipment, fuel, and personnel can be directed to where they are most needed.

3. Our experience over the years with major outages—from the 2017 hurricanes, tornadoes, and flooding, to power shutdowns in California and the latest earthquakes in Puerto Rico—all underscore the value of reliable and timely outage information to the rapid restoration of communications (including wireline and wireless telephone, television, radio, and satellite). This experience has also heightened our understanding of the crucial role state and local authorities can play in the successful restoration of disrupted communications. We thus now consider how more direct access to outage information might improve the situational awareness and ability of state and local authorities to respond more quickly to outages impacting their communities and to help save lives. Specifically, this Second Further Notice of Proposed Rulemaking proposes an information sharing framework that would provide state and federal agencies with access to NORS and DIRS information while also preserving the confidentiality of that data.

II. BACKGROUND

4. In 2004, the Commission adopted rules that require outage reporting for certain communications 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.” 69 FR 68859 (Nov. 26, 2004) (*2004 Part 4 Report and Order*).

5. Under these rules, certain service providers must submit outage reports to NORS for outages that exceed specified duration and magnitude thresholds. 47 CFR 4.9. Service providers are required to submit a notification into NORS generally within 30 minutes 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. 47 CFR 4.11.

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 to, in the short-term, assess the magnitude of major outages, and in the long-term, 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 withheld from routine public inspection, 47 CFR 0.457(d)(vi), 4.2. The Commission grants read-only access to outage report filings in NORS to the NCCIC at DHS, but it does not currently 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 publicly shares limited analyses

of aggregated and anonymized data to collaboratively address industry-wide network reliability issues and improvements.

8. In the wake of Hurricane Katrina, the Commission established DIRS as a means for service providers, including wireless, wireline, broadcast, and cable providers, to voluntarily report to the Commission their communications infrastructure status and situational awareness information during times of crisis. 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, 84 FR 59937, 59959-60 (Nov. 7, 2019) (*Puerto Rico & USVI USF Fund Report and Order*). DIRS, like NORIS, 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 communications following disasters.

9. The Commission treats DIRS filings as presumptively confidential and limits the disclosure of information derived from those filings. The Commission grants direct access to the DIRS database to the NCCIC at DHS. The Commission prepares and provides aggregated DIRS information, without company identifying information, to the NCCIC, which then distributes the information to Emergency Support Function #2 (ESF-2) participants, including other units in DHS, during an ESF-2 incident. ESF-2 is led by DHS and composed by other participants, including the Department of Agriculture, Department of Commerce, Department of Defense, General Services Administration, Department of Interior, and the Federal Communications Commission. Agencies use the analyses for their situational awareness and for restoration priorities for communications infrastructure in affected areas. The Commission also provides

aggregated data, without company-identifying information, to the public during disasters.

10. In 2009, the California Public Utilities Commission (CPUC) filed a petition requesting that the Commission amend its rules in order to permit state agencies to directly access the Commission's NORS filings for outages filed in their respective states, *Petition of the California Public Utilities Commission and the People of the State of California*, ET Docket No. 04-35 (filed Nov. 12, 2009) (CPUC Petition). The Commission sought public comment on the CPUC's request.

11. In 2015, 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," 80 FR 34321, 34357 (June 16, 2015) (*2015 Part 4 NPRM*). 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'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, in the *2015 Part 4 NPRM*, the Commission sought comment on sharing NORS filings with federal agencies pursuant to certain safeguards to protect presumptively confidential information.

12. In the *2016 Order and Further Notice*, the Commission found that the record reflected broad agreement 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 Part 4 Order and Further Notice*). The Commission determined that providing state and federal government 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.” Finding that the record was not fully developed and that the “information sharing proposals raise a number of complex issues that warrant 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 state commissions and federal agencies in real time, keeping in mind the information sharing privileges already granted to DHS.

13. 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.

14. This Second Further Notice of Proposed Rulemaking is part of our overarching effort to promote the reliability and redundancy of communications service in the United States. For example, the Commission is undertaking a comprehensive re-examination of the Wireless Resiliency Cooperative Framework to ensure that it is meeting the needs of communities, with a particular focus on increasing wireless service provider coordination with backhaul providers and electric utilities. Two federal advisory committees to the Commission, the Broadband Deployment Advisory Committee (BDAC) and the Communications Security, Reliability, and Interoperability Council VII (CSRIC VII) are developing recommendations to improve broadband and broadcast resiliency, respectively. PSHSB conducted an investigation into the

preparations for and impact of 2018's Hurricane Michael on communications services and issued a report with recommendations to improve future recovery efforts. The Bureau also sent letters to wireless providers seeking information on their preparations for electric power shutoffs and wildfires in California, and it conducted outreach with communications and electric industry stakeholders to assess lessons learned.

III. DISCUSSION

15. Based on the record before us, the majority of commenters agree that sharing NORS and DIRS information with state and federal agencies—in a manner that preserves the confidentiality of that information—would provide important public safety benefits. Accordingly, we propose a framework for granting state and federal government agencies direct access to NORS and DIRS filings that will assist agencies in their efforts to keep the public safe while preserving confidentiality, ensuring appropriate access, and facilitating reasonable information sharing.

A. Sharing NORS filings with State and Federal Agencies

16. NORS filings contain timely information on communications service disruptions or outages impacting a provider's networks. For example, NORS filings may include useful information about the operational status of communications services or 911 elements that have been affected, as well as incident date, time, and location details. The Commission previously found that sharing NORS data with state and federal agencies would serve the public interest—provided that appropriate and sufficient safeguards were implemented. We now propose to reaffirm this finding and to refresh the record.

17. The Puerto Rico Telecommunications Bureau shared its experience in responding to Hurricane Maria in 2017, specifically that the outages impacted communication services for

the government agencies responsible for providing essential services. Further, the Puerto Rico Telecommunications Bureau strongly encouraged the Commission to grant state access to NORS so that the agency can coordinate assistance to companies and to emergency government agencies in order to restore communication services and assist its citizens. The Massachusetts Department of Telecommunications and Cable (Massachusetts DTC) in turn argues that state agencies need “timely, unrestricted access to accurate outage information in order to respond quickly and maintain public safety.” Massachusetts DTC supports state access to NORS, citing the specific challenges it faced in accessing accurate and reliable information during the nationwide CenturyLink outage in December 2018, which also disrupted 911 service throughout the state. Massachusetts DTC states that during the December 2018 outage, “misinformation was disseminated” regarding the extent of the state’s 911 outages.

18. We believe that subject to appropriate safeguards, giving qualified state and federal agencies NORS access would help restore affected communications and ultimately help save lives. To what extent are state or federal agencies’ efforts to ensure the safety of the public frustrated by the fact that information about communications outages is either difficult to obtain or unavailable? Have there been recent public safety incidents where state or federal agencies could have led a more successful response had they been granted direct access to NORS filings at the time of the incident? How would direct access to NORS filings have assisted in the response for such public safety incidents? Are there additional benefits associated with granting direct access to NORS that we should consider?

B. Sharing DIRS Filings with State and Federal Agencies

19. As with NORS data sharing, we propose sharing DIRS filings with eligible state and federal agencies. Unlike NORS filings, which provide a baseline measure for network

reliability in a jurisdiction prior to and after disasters, DIRS filings are focused on network status during disasters and in their immediate aftermath. As emergency management officials in California have reported, their currently available resources for identifying the status of communications networks reflect data gaps and inconsistencies at times, which make it difficult for officials to make informed emergency management decisions at the local level, such as identifying and knowing how to move the public of out danger and how to report “medically-difficult situations.”

20. DIRS filings, on the other hand, contain timely information about the operational status of service providers’ networks and the associated infrastructure equipment, typically submitted on a daily basis during disaster conditions. DIRS filings also reflect a snapshot of whether specific service provider infrastructure equipment is running on backup power or out of service, as well as the operational status of 911 call centers. As we have found in past communications outages following a disaster, information indicating which counties have a large percentage of its cell towers out of service can provide state authorities the situational awareness they need to appropriately address the communications needs of vulnerable populations in affected areas. After its experience with Hurricane Maria, the Puerto Rico Telecommunications Bureau shared that the DIRS information that it received from communication service providers, not available from the DIRS public reports, was helpful and future access to DIRS information would be an “essential tool” to coordinate assistance to the companies and emergency government agencies in order to restore communication services and assist citizens affected by an outage. For these reasons, we believe that sharing DIRS information with qualified state and federal agencies would help them to better direct their limited resources, including field staff, to areas of most need, thereby enhancing their communications response and recovery efforts in

times of disaster. Service providers who report in DIRS submit information as frequently as on a daily basis. Thus, the information submitted may often represent near-real time status updates on critical communications infrastructure inside the counties most devastated during a natural disaster like a category 5 hurricane or wildfire.

21. Moreover, because the Commission affirmatively waives mandatory NORS reporting requirements for service providers that voluntarily report in counties where DIRS is activated, DIRS sharing will provide more complete and actionable status of communications outages. As the Michigan Public Service Commission observed, a state agency would have an “incomplete picture of outages” without access to both NORS and DIRS whenever DIRS is activated.

22. We seek comment on our analysis and these anticipated benefits. To what extent would our proposal to share DIRS filings with state and federal agencies improve the effectiveness of response and recovery efforts during and after disasters and emergencies? Are there other, equally effective methods that state and federal agencies may already use to obtain communications status information on a daily basis, especially during and after a devastating event such as a hurricane or wildfire, that does not require access to DIRS? Conversely, what, if any, harms may arise from granting state and federal agencies access to DIRS information? Given that service providers may voluntarily report confidential information in DIRS, we seek comment on whether federal and state agency access to DIRS filings would in any way reduce service provider participation or diminish the level of detail that service providers submit in DIRS. To what extent would any such harms outweigh the benefits of sharing that information? Could those harms be mitigated through the implementation of the safeguards proposed below, and if so, to what extent?

C. Eligible State, Federal, and Tribal Nation Government Agencies

23. We believe that providing state and federal agencies, including Tribal Nation government agencies, access to NORS and DIRS information will help promote the timely restoration of communications in affected communities. However, access to NORS and DIRS must be balanced against a need to safeguard and protect the presumed confidentiality of that information. We therefore believe it is necessary to limit the types of agencies that are eligible to receive direct access to NORS and DIRS. We propose that direct access to NORS and DIRS be limited to agencies acting on behalf of the federal government (we note that the NCCIC of DHS already has direct access to NORS and DIRS information; we do not propose to modify the terms by which the NCCIC accesses this information), the fifty states, the District of Columbia, Tribal Nation governments, and United States territories (including Puerto Rico and the U.S. Virgin Islands) that reasonably require access to the information in order to prepare for, or respond to, an event that threatens public safety, pursuant to its official duties (i.e., agencies with a “need to know”). Henceforth, we use the term “state” in this *Further Notice* to broadly refer to any of the fifty states, the District of Columbia, tribal governments, and United States territories. For purposes of our proposal, we use the term “agency” to refer to any distinct governmental department, commission, board, office, or other organization established to fulfill a specific purpose or role, including a state public utility commission or state department of public safety. We also propose that NORS and DIRS information accessed by these agencies should only be used for public safety purposes. We believe that this proposal provides NORS and DIRS access to the agencies that are in the best position to use outage and infrastructure status information to promote public safety across their jurisdictions. We seek comment on our definition of “need to know” and on any objective criteria that would be sufficient or necessary for a state or federal

agency to establish that it satisfies the “need to know” standard. What supporting materials should a state or federal agency provide to the Commission to support its assertion that it has a “need to know” as a condition of access to the NORS and DIRS data? We seek comment on the public safety purposes for which eligible agencies may use NORS and DIRS information, as well as on our proposal to condition access to this information on its use for public safety purposes only.

24. While local agencies will not be able to access NORS and DIRS directly under our proposal, we note that these agencies generally fall within the oversight jurisdiction of state agencies that are eligible. Therefore, the local entities would be in a position to obtain NORS and DIRS filings or information from an affiliated state agency, on a case-by-case basis, provided that the state agency finds that the local entities have a “need to know” justification. We further believe this approach is necessary for a NORS and DIRS information sharing framework to be administrable by the Commission, as county and local eligibility would be likely to result in tens of thousands of applications for access, which would take significant time to process and place significant burdens on Commission staff. We seek comment on our proposal.

25. Are there reasons why local entities require direct access to NORS and DIRS filings, and if so, how could these filings be protected from improper disclosure in view of the extremely large number of such local entities in the nation? Are there other entities, besides the state and federal agencies that we have identified above, that also should be eligible to participate in the proposed information sharing framework? How can we best balance addressing the public safety need for enhanced situational awareness against the risk of inadvertent disclosure of NORS and DIRS information, particularly given the large number of local entities in the nation?

26. For example, should additional criteria be applied to determine whether a specific type of local entity (e.g., local alert-originating entities) should be granted direct access to NORS and DIRS filings? If so, what should those additional criteria be? Should we introduce additional criteria for state-level agencies, such as limiting access to certain types of state agencies (e.g., state public safety and emergency management departments)? Should we exclude from eligibility agencies located in states that have diverted or transferred 911/Enhanced 911 (E911) fees for purposes other than 911/E911? If so, how should we address conditions of access for states that have inadequately responded to Commission inquiries as to their practices for using 911/E911 fees? Relatedly, should the types of federal agencies eligible for direct access to NORS and DIRS filings be limited and if so, what criteria should we consider?

27. Tribal Nation Governments. We seek comment on our inclusion of Tribal Nation governments in today's proposed information sharing framework. Given the rural location of many Tribal Nation governments, there may be fewer providers offering service in Tribal lands and each piece of communications equipment may be more critical to maintaining connectivity. Does this consideration weigh in favor of different standards for determining whether Tribal Nation government agencies should be granted access to NORS and DIRS filings compared to the other government agencies described in today's proposal? If so, what alternative standards should we use to best tailor our proposal to Tribal Nation governments?

D. Confidentiality Protections

28. The Commission currently treats NORS and DIRS filings as presumptively confidential. This means that the filings and the information contained therein would be withheld from public disclosure, shared on a limited basis to eligible entities, and provided to others in summarized and aggregated form and only in narrow circumstances. We propose to

extend this policy by requiring that participating state and federal government agencies treat NORS and DIRS filings as confidential unless the Commission finds otherwise. For clarity, “eligible agencies” refers to agencies that qualify for direct access to NORS and DIRS under this proposal, while “participating agencies” refers to agencies that have applied for and been granted direct access by the Commission.

29. We continue to believe that NORS filings should be presumptively confidential due to the “sensitive data” they contain that “could be used by hostile parties to attack . . . networks, which are part of the Nation’s critical information infrastructure.” We also continue to believe that DIRS filings should be presumptively confidential “[b]ecause the information that communications companies input to DIRS is sensitive, for national security and/or commercial reasons.” We remain concerned that our national defense and public safety goals could be undermined if information from outage reports could be used by malicious actors to harm, rather than improve, the nation’s communications infrastructure.

30. Further, we continue to be sensitive to the notion that the public disclosure of the NORS information, and more likely, the public disclosure of voluntarily submitted DIRS information, could make “regulated entities less forthright in the information submitted to the Commission” due to the “likelihood of substantial competitive harm from disclosure” of their submitted outage or infrastructure status information. We seek comment on these views and on any alternative approaches. We note that some service providers have recently announced plans to publicly release outage information not previously disclosed. We seek comment on the status of current policies, as well as any future plans, of service providers with regard to publicly releasing outage and infrastructure status information, including specific details as to the types of information that providers intend to release and the circumstances under which they will release

it. Verizon has argued that “increased public disclosure of company-specific outage information will further improve information flow and transparency during disasters and other emergencies without compromising competitively sensitive data.” We seek comment on how this argument should affect our views on the presumption of confidentiality afforded to NORS and DIRS data.

31. Moreover, we seek to provide confidence to NORS and DIRS filers that the information they submit would continue to be protected against public disclosure at its current level and to ensure consistency in the information that is publicly disclosed. We believe that a uniform confidentiality standard for granting state and federal agencies access to NORS and DIRS filings would help secure these results. We therefore propose that a participating agency’s direct access to NORS and DIRS filings be conditioned on the participating agency agreeing to treat the filings as confidential and not disclose them absent a finding by the Commission that allows them to do so. We propose that participating agencies that seek to disclose information would request the Commission’s review, which would occur in the same manner that the Commission reviews requests for disclosure under FOIA. This proposal mirrors the way in which federal agencies share homeland security information with state governments under section 892 of the Homeland Security Act of 2002, in which the federal agency remains in control of the information and state law that otherwise authorizes disclosure of information does not apply, 6 U.S.C. 482(e). We believe that our proposal would limit distribution of the information for unauthorized purposes, ensure the security and confidentiality of the information, and protect the rights of companies that submit the information. We seek comment on this approach.

32. We seek comment on alternative proposals that may address confidentiality concerns. Do any states have substantially different disclosure standards than federal FOIA and,

if so, would this condition be satisfied in jurisdictions with more permissive state open record laws or with court decisions favoring more permissive disclosure? We note that the Commission has dealt with similar issues before. With respect to competitively sensitive information submitted by carriers with respect to the North American Numbering Plan, the Commission recognized that some states had open record laws that might not allow state public utility commissions to protect the information from public disclosure. The Commission stated that it would work with those commissions to enable them to obtain the information they needed while protecting the confidential nature of the information. We acknowledge that in all cases, agencies would need to determine whether they can certify to the Commission that the agency would uphold the confidentiality protections we propose. We seek comment on whether these approaches are appropriate and workable here. Should the Commission rely on additional procedures to protect confidential materials from public disclosure by participating state or federal government agencies in this context?

33. To further ensure consistency in disclosure and confidence that submitted information will continue to be protected as it is today, we also propose to require participating state and federal agencies to notify the Commission on issues related to confidentiality in two instances. First, we propose that state and federal agencies notify the Commission within 14 calendar days from the date the agency receives requests from third parties for NORS filings and DIRS filings, or related records. This would provide the Commission the ability to notify the original NORS or DIRS submitter and give them an opportunity to object. Second, we propose that state and federal agencies notify the Commission at least 30 calendar days prior to the effective date of any change in relevant statutes or rules that would affect the agency's ability to adhere to the confidentiality protections that we require. This would 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, before the agency is no longer in a position to protect this information. We seek comment on this approach or on any alternative approaches that may achieve the stated goals.

E. Proposed Safeguards for Direct Access to NORS and DIRS Filings

1. Read-Only Direct Access to NORS and DIRS

34. We believe that agencies should receive access to NORS and DIRS in a format that reduces or eliminates the risk that their employees would make unauthorized modifications to the filings, whether unintentional or malicious. The current NORS database only allows users assigned to a company to modify reports submitted by that company. Preventing such modifications would ensure the accuracy of the Commission's oversight work and that of its partners, who rely on the accuracy of NORS and DIRS filings at all times. We thus renew our proposal that participating state and federal agencies be granted direct access to NORS and DIRS filings in a read-only manner. Many commenters to the [2015 Part 4 NPRM](#) supported a read-only access approach. For example, Verizon stated that "limit[ing] access to read-only format is [an] appropriate safeguard" based on "public safety, security, and competitive sensitivities." We seek further comment on the proposed read-only approach. Have any developments occurred since 2015, when we proposed to grant state governments read-only access, that weigh in favor or against providing access in a read-only manner? In addition, we currently require each user account in NORS and DIRS to use a password to access the systems. We seek comment on whether we should implement other technology protections to prevent unauthorized access to these databases given today's proposal, which would expand the number and scope of individuals with access to NORS and DIRS.

35. We believe that providing participating agencies with direct access to historical NORS and DIRS information would allow them to identify trends in outages and infrastructure status that would further enhance their real-time recovery and restoration efforts. We thus propose to grant participating agencies access to 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. Historical information will allow agencies to determine outage and infrastructure status baseline levels in their jurisdictions and identify trends, so that they can better predict and respond to emerging exigencies more rapidly than would otherwise be possible. We propose to limit access agency access to filings made after the effective date of this framework to address potential concerns that service providers may have about a potential dissemination of filings that they originally made to the Commission under an expectation that we would keep the filings presumptively confidential and withhold them from disclosure, even from federal and state government agencies that might seek them.

36. Are there reasons why we should not provide an agency access to filings after the effective date and prior to their participation in the proposed framework? Are there reasons that we should provide access to all historical filings that can be made available or, instead, that are made as of the date of today's proposal? The Commission estimates internal costs of approximately \$50,000 to revise its NORS and DIRS processes to ensure the compatibility of the NORS and DIRS databases with historical (e.g., non-multistate) filings. We seek comments on these costs. Alternatively, should participating agencies' access to NORS and DIRS information be limited to timeframes relevant to specific disasters or other events that threaten public safety for which those agencies are contemporaneously preparing or responding?

2. Sharing of Confidential NORs and DIRS Information

37. We recognize that, in many cases, there are individuals, including key decision-makers and first responders, who would not directly access NORs and DIRS and yet play a vital role within their respective jurisdictions in ensuring public safety during times of crisis. We believe there would be significant benefit in ensuring that these individuals also have access to the information in NORs and DIRS filings, in whatever form is most useful to them in furtherance of their duties. Accordingly, for each participating state or federal government agency, we propose to allow individuals granted credentials for direct access to NORs and DIRS filings to share copies (e.g., printouts) of NORs and DIRS filings, in whole or part, and any confidential information derived from NORs or DIRS filings (collectively, confidential NORs and DIRS information), within or outside their participating agency, on a strict “need to know” basis. Confidential NORs and DIRS information may include, as illustrative examples, presentations, e-mail summaries, and analysis and oral communication reflecting the content of, or informed by, NORs and DIRS filings. We also propose to require that this information be used for public safety purposes only.

38. A “need to know” basis exists where the recipient would need to reasonably require access to the information in order to prepare for, or respond to, an event that threatens public safety, pursuant to the recipient’s official duties. We propose that the sharing of confidential NORs and DIRS information be allowed “downstream” as well, meaning that once an agency with direct NORs and DIRS access shares confidential NORs and DIRS information with a recipient, that recipient can further summarize and/or share the information with others who also have a “need to know.” To ensure that non-participating agencies maintain the confidentiality of NORs and DIRS information, we propose to require that participating agencies

condition access to this information on non-participating agencies' certification that it will treat the information as confidential, not disclose it absent a finding by the Commission that allows them to do so, and securely destroy information when the public safety event that warrants their access to the information has concluded. We propose to hold participating agencies responsible for inappropriate disclosures of NORIS and DIRS information by the non-participating agencies with which they share it and expect that participating agencies will take all necessary steps to have confidence that confidentiality will be preserved. We also note that individuals or agencies that make inappropriate disclosures of NORIS in DIRS information may be subject to disciplinary action and/or liability under federal, Tribal and/or state laws that protect data, containing, e.g., trade secrets or other commercially sensitive information. We seek comment on any federal and non-federal restrictions that may apply to the improper dissemination of private information by employees of participating agencies and those with whom they share NORIS and DIRS information, and the consequences of violating them.

39. We seek comment on this approach of participating agencies agreeing to be held responsible for downstream information sharing as a pre-requisite for accessing NORIS and DIRS information. Would the measures proposed be sufficient to ensure that downstream recipients preserve the confidentiality of NORIS and DIRS information they receive? Relatedly, we seek comment on state laws and penalties would be sufficient to deter any inappropriate disclosure of NORIS/DIRS information. If these measures and state laws are not sufficient, we seek comment on any additional measures that we should include to ensure that confidentiality is maintained when sharing NORIS and DIRS information downstream. For example, to what extent should the Commission hold downstream recipients responsible when NORIS and DIRS information is improperly disclosed and what should the consequences be (apart from, for instance, immediate

cut-off of access for the agency that accessed the NORS and DIRS filings)? To what extent would additional measures hinder the ability of first responders and other emergency response officials to receive critical information, thereby undermining their restoration and recovery efforts? Are there measures we can take that would adequately preserve the confidentiality of information that was earlier shared downstream after the public safety event that necessitated sharing is over? We seek comment on the public safety purposes for which downstream recipients may use NORS and DIRS information, as well as on our proposal to condition access to this information on its use for public safety purposes only.

40. We propose that the sharing agency determine whether a “need to know” exists on the part of the recipient. We believe that the sharing agency is in a strong position to make this determination based on their “on the ground” knowledge of the public safety-related activities of agencies that are not eligible to access NORS and DIRS directly. Moreover, we find that it would be impractical for Commission to either make these case-by-case determinations, which would often be made during on-going exigencies.

41. Under our proposals, confidential NORS and DIRS information could be shared when the recipient has a “need to know” basis, for example, in the following illustrative scenarios:

- (a) an employee with direct NORS and DIRS access in a participating agency may share confidential NORS and DIRS information within any number of agency employees or contractors (e.g., a public utility agency may share information among its employees and contractors to resolve a power outage situation);
- (b) an employee with direct NORS and DIRS access in a participating agency may share confidential NORS and DIRS information with the employees and contractors of other

participating or non-participating agencies within the same state/jurisdiction or in a different state/jurisdiction (e.g., a public utility agency may share information with a neighboring state governor's office responding to a hurricane; or a state emergency management agency may share information with a region-level fire chief);

(c) an employee at a non-participating agency who receives the confidential NORs and DIRS information on a "need to know" basis may then share the information with an employee at another non-participating agency based on the latter's "need to know" (e.g., a region-level fire chief may share information with a county sheriff's department for the purpose sending first responders to an affected area).

We seek comment on this proposal, as well as on other ways to permit sharing of NORs and DIRS information by participating agencies when such sharing helps to address public safety issues.

42. Does our approach provide sufficient benefits to key decision-makers and first responders to outweigh the risk of potential over-disclosure of confidential information? What additional steps can we take, if any, to mitigate such risks while preserving the benefits? What would be the burden to participating agencies and others if we were to take additional steps? For example, should we require, as a condition for access to the data, that participating agencies notify the Commission when they share NORs and DIRS information with a downstream recipient, and if so, what form should the notification take? Should notification include specific information on which individuals, localities, and Tribal lands are receiving this information downstream and describe the basis for any "need to know" determinations? Should notification be provided to the Commission within a certain timeframe after the sharing occurs? Alternatively, in order to ensure that participating agencies' focus during a public safety event

remains on response and restoration, should notification be provided to the Commission in advance in the form of a list of those downstream agencies with which it is anticipated the information will be shared? For such an approach, we seek comment on whether, in the event there is an exigency that necessitates sharing with agencies that were not on the advance list, participating agencies should be given a certain period of time to notify the Commission of additional downstream agencies with which the information was shared?

43. What steps can we take to ensure that agencies are handling and sharing confidential information appropriately? Are there reasons why downstream sharing or sharing outside an agency should be more limited than described here? Should we adopt further measures to control or limit the downstream sharing of confidential NORs and DIRS information beyond the specific individuals with direct access, and if so, what specific measures should we adopt and what should be the consequences if they are not followed? On the other hand, should downstream agencies without access to NORs and DIRS be allowed to keep NORs and DIRS data, perhaps to allow it to be studied in an after-action review of their response efforts? To the extent that commenters recommend less or more restrictive frameworks (including ones that nonetheless facilitate broader sharing in emergency situations), we request that commenters identify in detail how such mechanisms would work, as well as their benefits and costs.

3. Disclosing Aggregated NORs and DIRS Information

44. We believe that the aggregated information in NORs and DIRS filings can be of significant benefit to the general public. For example, this information can be used to keep the public informed of on-going emergency and network outage situations, timelines for recovery, and geographic areas to avoid while disaster and emergency events are ongoing. We therefore

propose to allow agencies to provide aggregated NORS and DIRS information to any entity including the broader public (e.g., by posting such information on a public website).

45. We define “aggregated NORS and DIRS information” 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. We seek comment on this approach and whether there are other appropriate aggregation requirements that we should consider. For example, should we require aggregation over a larger number of service providers? We note that allowing the public disclosure of aggregated NORS and DIRS information is consistent with the Commission’s own practices.

46. Here, we propose extending the ability to generate and supply aggregated NORS and DIRS information to participating state agencies themselves. We believe that granting participating agencies this flexibility will allow them to disseminate information to the broader public and better fulfill their public safety missions. Moreover, we believe that this proposal carries at most a minimal risk of the over-disclosure of sensitive information since participating agencies must anonymize aggregated NORS and DIRS information. We seek comment on this proposal. Are there any specific steps that agencies should take beyond aggregating over four or more providers to ensure that NORS and DIRS information is adequately aggregated and anonymized prior to disclosure? Should we adopt specific measures to ensure that, as a condition of access to NORS and DIRS filings and information, participating agencies adequately aggregate and anonymize the information in NORS and DIRS filings and information prior to disclosure? If so, what should those measures be and what should be the consequences if they are not followed?

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

47. We observe that an outage or a disaster—such as a hurricane—may cross multiple jurisdictional boundaries. We believe that agency access to NORS and DIRS filings should account for this reality. We propose that a participating agency 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. For federal agencies, this generally means for events reported to occur anywhere in the country. For state agencies, this generally means for the events reported to occur at least partially in the state’s geographic boundaries. Commenters support granting states access to NORS filings and DIRS filings for events that occur within their jurisdiction. We propose that it would serve the public interest for participating state agencies to access NORS and DIRS filings for outage events and disasters that occur in portions of their respective state but also span across additional states.

48. We seek comment on this proposal. How would participating agencies make use of NORS and DIRS filings that affect states beyond their own? Do participating agencies have a “need to know” about the effects of multistate outages and infrastructure status outside their jurisdiction? Do county or local agencies that cannot access NORS and DIRS under our proposal have similar needs? What benefits are expected to arise from granting participating state agencies access to these NORS and DIRS filings? Are there any harms that may potentially arise from granting participating state agency access to multistate outage and infrastructure information? As an alternative to our proposal, should participating agencies’ access to NORS and DIRS filings be limited only to those aspects of multistate outages that occur solely in their jurisdiction? Are there specific aspects of multistate outages for which participating agencies do not have a “need to know?” In addition, we anticipate that there may be situations where a

participating agency may share confidential information derived from DIRS or NORS filings with non-participating state or federal agencies on a strict “need to know” basis. We seek comment on this view.

49. Does a participating federally recognized Tribal Nation’s government agency that receives direct access to NORS and DIRS filings have a “need to know” about events that occur entirely outside of its borders but within the border of one the state where the Tribal land is located? For example, should a participating Tribal Nation agency located in Arizona receive direct access to filings throughout all of Arizona? Conversely, should a state agency receive direct access to NORS and DIRS filings reflecting events occurring entirely within Tribal land located in the state’s boundaries? For example, should a participating Arizona state agency receive direct access to NORS and DIRS filings for outages occurring only within Tribal lands located in Arizona? We believe that both aspects of this approach are justified given the technical nature of many outages, where equipment located in a Tribal land affects service in the traditional state(s) surrounding the territory, and vice versa. We seek comment on this approach. Are there any harms that may potentially arise from granting Tribal Nation authorities access to outage and infrastructure information outside of their territories? As an alternative to our proposal, should Tribal Nation authorities’ access to NORS and DIRS filings be limited only to those aspects of multistate outages that occur solely in their territories? Are there specific aspects of multistate outages for which these authorities do not have a “need to know?”

50. We seek comment on the technical implementation of our proposals. Since the DIRS form already requests filers to include data at the county level, we do not anticipate that service providers will need to modify their DIRS reporting processes to accommodate multistate reporting. We thus estimate that the nation’s service providers will incur minimal, if any,

burdens related to DIRS. We seek comment on this assessment.

51. For NORS filings, however, commenters raise concerns that sharing filings with state agencies will require technical adjustments for both the service providers' systems and the Commission's internal systems. For example, the current NORS forms are designed with a drop-down menu for a user to select the state where the outage occurred. A NORS user may select either a single state or the general option of "MULTI STATE" in the current form without specifying the individual states. This existing approach makes it challenging to identify which multistate outage filings each participating state agency should have permission to access. As Intrado noted previously, in order to filter and display the NORS filings that pertain to any given state, including multi-outage filings, the NORS form would require adjustments.

52. We propose to change the Commission's NORS form to allow users to select more than one state when submitting a NORS filing. This approach will allow us to limit state agencies' access to only those outages that occur within their states. We expect that service providers will need to make corresponding changes to their NORS reporting processes to provide us with information on a state-by-state basis. We currently estimate that the nation's service providers will incur total initial set up costs of \$3.2 million based on our estimate of 1,000 service providers incurring costs of \$80 per hour and spending 40 hours to update or revise their software used to report multi-state outages to the Commission in NORS. In developing this analysis, the Commission estimates that the cost of a software developer of systems software is \$80/hour, inclusive of wage and benefits. We seek comment on the burden and timelines associated with such modifications. We seek comment on whether the benefits associated with these modifications would outweigh the costs incurred by service providers.

53. We seek comment on this approach, as well as on any potential alternatives,

including any adjustments, if needed, to account for Tribal land borders. For example, we seek comment on whether, instead of modifying the NORS form, we should require service providers to submit several state-specific filings instead of submitting single aggregated filings for each outage that list all affected states.

5. Limiting the Number of User Accounts Per Participating Agency

54. We believe that it would be beneficial to limit the number of users at an agency who have access to NORS and DIRS filings to minimize the potential for over-disclosure of the sensitive information contained in the filings. At the same time, we recognize that agencies typically employ teams of staff members, rather than a lone individual, to provide “around the clock” coverage for incident response. We propose to presumptively limit the number of user accounts granted to a participating agency to five NORS and DIRS accounts per state or federal agency with additional accounts permitted on an agency’s reasonable showing of need. We further propose to require 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 (e.g., due to arrivals and departures or a change in roles at the participating agency). We believe that these requirements 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.

55. We seek comment on this approach. For example, are there reasons why the Commission, rather than participating agencies, should be responsible for assigning individualized user accounts, i.e., accounts corresponding with specific named employees, and for re-assigning user accounts as participating agency personnel changes with time? We observe that AT&T, based on concerns for safeguarding the commercially and national security-sensitive nature of NORS information, proposed a similar approach, suggesting that we impose a limit of

“three individuals unless the state can provide adequate justification for more employees.” We agree with a presumptive limit, but we believe that the presumptive limit should be at least five employees, given our understanding of the size and complexity of network monitoring and emergency response operations at many state and most federal agencies. Other commenters to the 2015 Part 4 NPRM generally support limiting the number of direct access users to NORS.

56. We recognize that some agencies—such as federal agencies or state agencies responsible for large populations or coverage areas—may have a reasonable need to provide more than five employees with direct access to fulfill their public safety mandate. Thus, we propose to consider, on a case-by-case basis, an agency’s request to increase their limit upon written request to the Commission specifying how many additional employees require access and providing specific reasons why their access is necessary. We propose to grant such requests upon an agency’s reasonable showing of need. We seek comment on this approach. Would this approach provide such agencies with sufficient flexibility, or should we establish a different presumptive limit for federal agencies or state agencies with the largest populations or coverage areas? Should there be a different presumptive limit of employees for agencies that serve a coverage area or population above a certain size? If there should be a different presumptive limit, what presumptive limit and qualifying size would be appropriate to ensure the confidentiality of the information provided NORS and DIRS filings? Are there additional or alternative criteria that the Commission should use to evaluate requests?

57. We believe that multiple state and federal agencies often need to collaborate on issues such as disaster response, operating with jurisdictional boundaries that may not always be clearly demarcated under challenging and time-constrained circumstances. For this reason, we propose that the Commission review all reasonable requests from state and federal agencies,

rather than proposing a presumptive limit on the number of participating state and federal agencies eligible for direct access to NORS and DIRS filings. Given the important and time sensitive work of these agencies, we seek to reduce the reliance of any one agency on another by allowing each to apply for direct access to NORS and DIRS filings. We seek comment on this proposal.

6. Training Requirements

58. We believe that our proposed sharing framework would be more effective, and the risk of over-disclosure of NORS and DIRS information minimized, if individuals who receive direct access to NORS and DIRS filings also receive training on their privileges and obligations under the program, particularly given that NORS and DIRS filings implicate both national security and commercial interests. We believe that an annual training requirement is justified both generally as an industry standard practice and because there are a number of important procedural details associated with our proposed safeguards that could be easily forgotten and overlooked with time in the absence of continued training.

59. For each participating agency, we propose that each individual to be granted a user account for direct access to NORS and DIRS filings be required to complete security training on the proper access to, use of, and compliance with safeguards to protect these filings. We propose that this training be completed by each individual prior to being granted initial access to NORS and DIRS filings and then on at least an annual basis thereafter.

60. Rather than mandate an agency's use of a specific program, we propose to allow agencies to develop their own training program or rely on an outside training program that covers, at a minimum, each of the following topics or "program elements": (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 e-mail 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. We seek comment on this proposal, including each of the elements.

61. The majority of commenters who opined on the issue of training believe that some form of training is necessary. For example, AT&T stated that the “[C]ommission should require states to train their authorized employees (annually) on proper handling of NORS information,” and Sprint stated that “[t]he Commission should require that personnel charged with obtaining the information be required to have security training, and the identity of these individuals should be supplied to the FCC.” We acknowledge that a minority of commenters believe that training is not necessary. Contrary to the concerns expressed by some of these commenters, we are not proposing to require that any state or federal agency participate in the proposed sharing framework. Rather, participation by an agency would be entirely voluntary. Further, to the extent training costs are an issue for a participating agency, we propose to reduce the agency burden through the use of exemplar training programs.

62. To aid agencies' compliance with our training requirements, we propose that the Commission direct PSHSB to identify one or more exemplar training programs which would satisfy the required program elements. Once finalized, agencies could adopt these program(s) at

their discretion in place of developing their own training program, thereby reducing their compliance time and costs. ATIS suggested that an exemplar-type training program could be developed (by its Network Reliability Steering Committee) in a matter of “months” once the Commission issues information sharing rules. We seek 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(s).

63. We seek comment on whether the Commission should take steps to ensure that state and federal agencies’ training programs comply with our proposed required program elements. Should the Commission require a third-party audit of a partner-developed training program? What specific steps should the Commission take, if any, to ensure the adequacy of such programs? We seek comment on whether additional individuals, beyond those granted a user account for direct access to NORS and DIRS filings, should be subject to the proposed training requirements. Should anyone who receives confidential NORS and DIRS information, including downstream recipients, be required to complete formal training? Would such a requirement be practical or overly burdensome? If we impose such a requirement, what should the consequences be if that training is not provided?

F. Procedures for Requesting Direct Access to NORS and DIRS

64. We believe that our proposed information sharing framework would be more effective, and the risk of over-disclosure of NORS and DIRS information minimized, if we institute specific procedures for state and federal agencies to follow in applying for and managing their direct access to NORS and DIRS filings. We believe that these goals would also be furthered if we require that agency representatives provide a signed certification acknowledging their agreement to adhere to the key safeguards of our proposed framework.

65. We therefore propose to institute the following procedures for state and federal agencies to apply for and manage their direct access to NORS and DIRS filings. Eligible state and federal agencies must apply for direct access to NORS and DIRS filings by sending a request to the agency's designated e-mail address. 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.

66. As described in detail at Appendix C, an agency official with authority to obligate and bind the agency must certify that the agency: will treat NORS and DIRS filings and data as confidential under federal and state FOIA statutes and similar laws and regulations, implement a NORS and DIRS security training program, adhere to continuing requirements for access (including annual recertification), understands that the Commission does not guarantee the accuracy of NORS or DIRS filings and understands that there may be times access to the filings is unavailable. We believe that these requirements would create accountability within a state agency and help avoid the over-disclosure of sensitive NORS and DIRS information sharing

framework. We seek comment on this approach and the details included in Appendix C. Is our requirement, set forth in Appendix C, that the Commission be notified if an agency's certifying official ceases to have authority to obligate and bind the agency to the provisions of Appendix C justified or would this requirement cause undue burden for an agency?

67. In addition, we propose to direct PSHSB to promulgate any additional procedural requirements that may be necessary to implement our proposals for the sharing of NORs and DIRS information, consistent with the Administrative Procedure Act. 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. We seek comment on these proposals, and whether there are additional safeguards we should adopt for the application process. Are there other procedural requirements that are anticipated to be necessary to implement our proposals?

G. Compliance Dates

68. We seek to give interested state and federal agencies ample time to prepare their certifications and to give service providers sufficient time to adjust their NORs and DIRS filing processes to conform with the any technical changes required by the proposed final rule changes. We also anticipate that the Commission will require time to implement the regime contemplated by our proposed rules in order to take such steps as securing OMB approval to the extent required under the Paperwork Reduction Act and modifying NORs and DIRS.

69. To that end, we propose to require revised outage reports be filed by a date specified in a Public Notice issued by the Public Safety and Homeland Security Bureau,

announcing: (i) OMB has approved the revised information collections for DIRS and NORS, respectively, in accordance with the final order; and (ii) the Commission has made the necessary technical adjustments to the NORS and DIRS databases to facilitate sharing. The Commission would begin accepting certification forms and granting direct NORS and DIRS access to eligible state and federal agencies as of the specified date. This approach would permit the Bureau to account for the contingencies, i.e., the readiness of the databases and the OMB approval that facilitates the implementation of the revised regime. We seek comment on this approach, as well as alternatives. Commenters proposing alternatives should explain the advantages and disadvantages of their preferred approaches.

IV. PROCEDURAL MATTERS

70. *Paperwork Reduction Act.* This document contains proposed modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Pub. L. 104 through 13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Pub. L. 107 through 198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

71. *Ex Parte Rules - Permit-But-Disclose.* This proceeding shall be treated as a “permit-but-disclose” proceeding in accordance with the Commission’s *ex parte* rules, 47 CFR 1.1200 *et seq.* Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons

making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with Rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

V. INITIAL REGULATORY FLEXIBILITY ANALYSIS

72. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the Further Notice of Proposed Rule Making (*Further Notice*). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments provided in "Comment Period and Procedures" of the *Further Notice*.

A. Need for, and Objectives of, the Proposed Rules

73. The *Further Notice* seeks additional comment on various proposals first issued in a Notice of Proposed Rulemaking in PS Docket No. 15-80, adopted in 2015, and a Report and Order and Further Notice of Proposed Rulemaking in PS Docket Nos. 15-80 and 11-82, adopted in 2016, to update the Commission's part 4 outage reporting rules. More specifically, in the *Further Notice* the Commission proposes an information sharing framework to ensure that state and federal government agencies have access to communications network information to aid these agencies' response, recovery and restoration efforts and allow them to direct their resources quickly, and to the areas of greatest need.

74. The proposals in the *Further Notice* to grant participating agencies of the states, the District of Columbia, Tribal Nations, territories, and the federal government (we note that the NCCIC of DHS already has direct access to NORS and DIRS information; we do not propose to modify the terms by which the NCCIC accesses this information), hereinafter agencies, direct access to outage and infrastructure status information establish safeguards to protect the confidentiality of Network Outage Reporting System (NORS) and Disaster Information Reporting System (DIRS) filings. The Commission's proposals define the scope of eligible government entities that would be able to participate and propose confidentiality protections that include requiring that NORS and DIRS data be treated as presumptively confidential. The proposals consider providing read-only access, limiting access based on agency jurisdiction, limiting the number of employees with access at each agency, requiring training requirements for employees with access, and specifying procedures for the sharing of confidential NORS and DIRS information. The proposed rules also include access request and certifications procedures for agencies to apply for and manage their direct access NORS and DIRS filings.

75. The *Further Notice* seeks further comment on a number of the implementation details for proposed agencies' direct access to NORS and DIRS filings. To establish appropriate safeguards, the *Further Notice* specifically seeks comment on:

- Providing agencies with read-only access to NORS and DIRS filings to reduce the potential for unauthorized modifications;
- Presumptively limiting the number of identified and trained personnel that have direct access to NORS and DIRS filings by limiting the number of user accounts to five per agency;
- Requiring agencies to treat NORS and DIRS filings and data as confidential under federal and state FOIA statutes and similar laws and regulations;
- Requiring each individual granted a user account for direct access to NORS and DIRS filings complete security training on the proper access to, use of, and compliance with safeguards to protect the information contained in the filings;
- Limiting agency access to NORS and DIRS filings for events reported to occur at least partially within their jurisdictional or geographic boundaries;
- Allowing participating agencies to share confidential NORS and DIRS information inside or outside the agency if a recipient reasonably requires access to the confidential NORS and DIRS information to prepare for, or respond to, an event that threatens public safety, pursuant to the recipient's official duties;
- Allowing participating agencies to share information from the NORS and DIRS filings of at least four service providers that has been aggregated and anonymized to avoid identifying any service provider by name or in substance with any entity, including the broader public; and

- Requiring agencies to provide certain assurances and suitable attestation that they will take measures to protect NORS and DIRS filings from unauthorized access.

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

76. 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 proposed rules, if adopted. 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). See 15 U.S.C. 632. Below is a list of such entities.

- Interconnected VoIP services;
- Wireline Providers;
- Wireless Providers – Fixed and Mobile;
- Satellite Service Providers; and
- Cable Service Providers.

C. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements

77. We expect the proposed rules in the *Further Notice* will impose new or additional reporting or recordkeeping and/or other compliance obligations on service providers, and if they choose to participate, on agencies that are granted direct access to NORS and DIRS filings, and these entities may have to hire professionals to fulfill their compliance obligations. The rules

proposed in the *Further Notice* would require minor adjustments to the existing reporting process used by service providers to account for new or refined multistate reporting for the NORS and DIRS filings. We estimate that service providers will incur total initial set up costs of \$3.2 million based on our 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. We seek comment on costs to service providers associated with any updates or modifications to their automated software and other systems that would be required for them to continue to file NORS reports under our proposed information sharing framework.

78. Pursuant to the proposed confidential protections, if adopted, voluntarily participating agencies 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. We believe these agencies would incur initial costs to review and revise their confidentiality protections in accordance with the proposed information sharing framework and minimal reoccurring costs to notify the Commission about a request for NORS/DIRS filings or relevant statutory changes as described above. The Commission cannot quantify the costs for these activities, which would vary based on each participating agency's particular circumstances, however, we tentatively conclude that the benefits of participation would exceed the costs for any participating agency and seek comment on these matters.

79. Under the proposed information sharing framework, voluntarily participating agencies will be required to submit to the Commission requests for direct access to NORS and DIRS filings which includes 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. These agencies will also be required to administer annual security training to each person granted a user account for NORS and DIRS filings. 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 within 24 hours of the breach or suspected breach. The Commission believes these participating agencies will incur costs to comply with the above requirements, however, we cannot quantify the costs for these activities, which would vary based on each participating agency's particular circumstances, however, we tentatively conclude that the benefits of participation would exceed the costs for any participating agency and seek comment on these matters.

80. In the *Further Notice*, the Commission proposes to allow participating agencies to share confidential NORS and DIRS information within and outside the agency subject to certain limitations. A participating agency would likely incur initial costs to determine how to appropriately handle and disseminate confidential NORS and DIRS information consistent with the proposed information sharing framework. The *Further Notice* also proposes to require participating agencies to execute an annual attestation form certifying and acknowledging compliance with requirements of the information sharing framework that the Commission adopts. These agencies will undoubtedly incur costs to comply these new requirements if adopted, but the Commission cannot quantify the costs for these activities, which would vary based on each participating agency's particular circumstances and therefore seeks comment on the matters.

D. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rule

81. None.

VI. LEGAL BASIS

82. Authority for the actions proposed in this Second Further Notice of Proposed Rulemaking may be found 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, 403, 615a-1, and 615c of the Communications Act of 1934, as amended, and section 706 of the Communications Act of 1996, 47 U.S.C. 151, 154(i) through (j) & (o), 251(e)(3), 254, 301, 303(b), 303(g), 303(r), 307, 309(a), 309(j), 316, 332, 403, 615a-1, 615c, and 1302.

List of Subjects in 47 CFR Part 4

Airports, Communications common carriers, Communications equipment, Disruptions to communications, Network outages, Reporting and recordkeeping requirements, Telecommunications, Federal Communications Commission.

FEDERAL COMMUNICATIONS COMMISSION

Cecilia Sigmund,
Federal Register Liaison Officer,
Office of the Secretary.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to be amend 47 CFR Part 4 as follows:

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

Authority: 47 U.S.C. 151, 154(i) through (j) & (o), 251(e)(3), 254, 301, 303(b), 303(g), 303(r), 307, 309(a), 309(j), 316, 332, 403, 615a–1, 615c, 1302, unless otherwise noted.

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, except that the Chief of the Public Safety and Homeland Security Bureau may grant agencies of the states, the District of Columbia, Tribal Nations, territories and federal governments access to portions of the information collections affecting their respective jurisdictions only after each requesting agency has certified to the Commission that it has protections in place to safeguard and limit disclosure of confidential information to third parties as described in the Commission's Certification Form. Public access to reports filed under this part may be sought only pursuant to the procedures set forth in 47 CFR 0.461. Notice of any requests for public inspection of outage reports will be provided pursuant to 47 CFR 0.461(d)(3).

[FR Doc. 2020-06085 Filed: 3/30/2020 8:45 am; Publication Date: 3/31/2020]