Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Charter Communications, Inc.	)	File No.: EB-SED-23-00035290
	)	CD Acct. No.: 202432100005
	)	FRN: 0023684756

ORDER

Adopted: July 29, 2024 **Released: July 29, 2024**

By the Chief, Enforcement Bureau:

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission) has entered into a Consent Decree with Charter Communications, Inc. (Charter) to resolve the Bureau's investigation into whether Charter violated the Commission's rules related to network outages, including those impacting 911 service. The failure to notify affected public safety answering points (PSAPs) of an outage impedes the ability of public safety officials to mediate the effects of an outage by notifying the public of alternate ways to contact emergency services. The failure to provide required outage notifications to the Commission through the Network Outage Reporting System (NORS) impairs the Commission's ability to assess the magnitude of major outages, identify trends, and promote network reliability best practices that can prevent or mitigate future disruptions. Therefore, it is imperative for the Commission to hold providers, like Charter, accountable for fulfilling these essential obligations. To settle this matter, Charter admits that it: (1) failed to timely notify more than 1,000 PSAPs of an outage on February 19, 2023 (Outage); (2) failed to meet reporting deadlines for reports in the NORS associated with the Outage, and separate outages on March 31 and April 26, 2023; and (3) failed to meet other NORS reporting deadlines associated with hundreds of planned maintenance outages, all in violation of the Commission's rules. Charter has agreed to implement a robust compliance plan, including cybersecurity provisions related to compliance with the Commission's 911 rules, and will pay a $15,000,000 civil penalty.

2. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest would be served by adopting the Consent Decree and terminating the referenced investigation regarding Charter's compliance with its obligations under sections 4.9 and 9.11 of the Commission's rules, including Charter's provision of notifications to PSAPs and to the Commission of network outages.[1]

3. In the absence of material new evidence relating to this matter, we do not set for hearing the question of Charter's basic qualifications to hold or obtain any Commission license or authorization.[2]

4. Accordingly, **IT IS ORDERED** that, pursuant to section 4(i) of the Act, 47 U.S.C. § 154(i), and the authority delegated by sections 0.111 and 0.311 of the Commission's rules, 47 CFR §§ 0.111, 0.311, the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

5. **IT IS FURTHER ORDERED** that the above-captioned matter **IS TERMINATED**.

[1] 47 CFR § 4.9.

[2] *See id.* § 1.93(b).

6. **IT IS FURTHER ORDERED** that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Maureen O'Connell, Vice President, Government Affairs, 601 Massachusetts Ave. NW, Suite 400 West, Washington, D.C. 20001, and Suzanne M. Tetreault, Wilkinson Barker Knauer, LLP, 1800 M Street NW 800N, Washington, D.C. 20036.

FEDERAL COMMUNICATIONS COMMISSION

Loyaan A. Egal
Chief
Enforcement Bureau

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Charter Communications, Inc.	)	File No.: EB-SED-23-00035290
	)	CD Acct. No.: 202432100005
	)	FRN: 0023684756

CONSENT DECREE

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission or FCC) and Charter Communications, Inc. (Charter or Company), by their authorized representatives, hereby enter into this Consent Decree for the purpose of terminating the Bureau's investigation into whether the Company violated the Commission's 911 Rules in connection with a network outage experienced by the Company on February 19, 2023 (Outage), two additional outages on March 31, 2023, and April 26, 2023, and hundreds of planned maintenance-related outages that Charter failed to report to the Commission. To resolve this matter, the Company agrees to the terms and conditions below, including an admission that it violated section 4.9(g) of the Commission's Rules requiring the timely notification of reportable outages to Public Safety Answering Points (PSAPs) and the filing of Network Outage Reporting System (NORS) reports with the Commission, the implementation of a robust compliance plan, and payment, in accordance with the terms hereof, of a $15,000,000 civil penalty.

I. DEFINITIONS

2. For the purposes of this Consent Decree, the following definitions shall apply:

(a) "911 Rules" means sections 4.9 and 9.11(b)(2) of the Rules, including the Notification Rules.[1]

(b) "Act" means the Communications Act of 1934, as amended.[2]

(c) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(d) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(e) "CD Acct No." means the account number 202432100005, associated with payment obligations described in paragraph 20 of this Consent Decree.

(f) "Charter" or "Company" means Charter Communications, Inc., and its subsidiaries, predecessors-in-interest, successors-in-interest, and assigns.

(g) "Commission" and "FCC" mean the Federal Communications Commission and all of its bureaus and offices.

(h) "Communications Laws" means collectively, the Act, the Rules, and the published and promulgated orders and decisions of the Commission, to which the Company is subject by virtue of its business activities, including but not limited to the 911 Rules.

(i) "Compliance Plan" means the compliance obligations, program, and procedures

[1] 47 CFR §§ 4.9, 9.11(b)(2).

[2] 47 U.S.C. § 151 et seq.

described in this Consent Decree at paragraph 16.

(j) "Covered Employees" means all employees and agents of the Company who perform, supervise, oversee, or manage the performance of, duties that relate to the Company's responsibilities under the 911 Rules.

(k) "Effective Date" means the date by which both the Bureau and the Company have signed the Consent Decree and the Bureau has released an Adopting Order.

(l) "Investigation" means the investigation commenced by the Bureau in File No. EB-SED-23-00035290.

(m) "Notification Rules" means section 4.9 of the Rules, and other Communications Laws governing the required notification to PSAPs about problems in the delivery of 911 calls, and the submission of Network Outage Reporting System (NORS) filings with the FCC.[3]

(n) "Operating Procedures" means the internal operating procedures and compliance policies established by the Company to implement the Compliance Plan.

(o) "Parties" means Charter and the Bureau, each of which is a "Party."

(p) "Rules" means the Commission's regulations found in Title 47 of the Code of Federal Regulations.

II. BACKGROUND

3. Section 4.9(g)(1)(i) of the Commission's Rules requires interconnected voice over Internet protocol (VoIP) service providers, in the event of an outage that "potentially affects a 9-1-1 special facility," to notify the designated official at the affected PSAPs of the outage "as soon as possible" and "convey to that person all available information that may be useful in mitigating the effects of the outage . . . " after discovering that they have experienced an outage of at least 30 minutes that potentially affects a special facility as defined in section 4.5(e).[4] Both late and never-filed notifications are violations of section 4.9(g)(1)(i). Likewise, section 4.9(g)(1)(i) requires interconnected VoIP service providers to timely file a NORS notification with the Commission within 240 minutes of discovering that the outage lasted at least 30 minutes and potentially affected a 911 special facility.[5] Interconnected VoIP service providers must follow up with the filing of a final report with the Commission within thirty days after discovering the outage.[6] Pursuant to section 4.9, providers are obligated to file NORS reports for all outages that meet the outage thresholds, irrespective of the cause,[7] with the Commission explicitly including planned maintenance within this scope.[8]

4. On February 19, 2023, Charter's network monitoring tools began to trigger alerts indicating problems with a portion of its voice infrastructure network.[9] It was determined that Charter's

[3] 47 CFR § 4.9.

[4] *Id*. § 4.9(g)(1)(i).

[5] *Id*. § 4.9

[6] *Id*. § 4.9(g)(2).

[7] *Id.* § 4.9.

[8] *See New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830, 16889, para. 114 (2004) (rejecting the contention that planned outages should not be reportable and concluding that, regardless of the reason for it, any outage that meets the threshold must be reported.)

[9] *See* Response to Letter of Inquiry, Counsel to Charter, Wilkinson Barker Knauer LLP, to Spectrum Enforcement Division, FCC Enforcement Bureau at 5-6 (July 31, 2023) (LOI Response).

network was the target of a minor, low and slow Denial of Service (DoS) attack.[10] As a result, Charter experienced an interconnected VoIP telephony service outage that affected approximately four hundred thousand (400,000) residential and commercial interconnected VoIP customers in portions of 41 states and the District of Columbia.[11] Charter was able to restore service in less than four (4) hours.[12] According to the Cybersecurity and Infrastructure Agency (CISA), "there is no way to completely avoid becoming a target of a DoS or DDoS attack… ."[13] Charter maintains that it adheres to CISA's best practices and the Cybersecurity Framework of the National Institute of Standards and Technology (NIST).[14]

5. The Outage met the section 4.9(g)(1) and (2) threshold for NORS reporting, but Charter failed to file the required NORS notification until almost six (6) hours after it was due.

6. Additionally, Charter was required to notify all of the impacted PSAPs "as soon as possible," but due to a clerical error associated with the sending of an email notification, over 1,000 PSAPs were not contacted.[15]

7. On June 1, 2023, the Bureau issued a Letter of Inquiry (LOI) to the Company directing it to submit a sworn written response to a series of questions relating to the Outage, and the Bureau issued follow-up questions on September 13, 2023, and October 19, 2023.[16] The Company timely responded to the LOI and to follow-up inquiries.[17]

8. As part of the investigation, EB asked Charter to identify and provide detail on other outages that met the NORS reporting threshold.[18] In response, Charter indicated that based on a misunderstanding of the Commission's rules, hundreds of planned maintenance events may have met the criteria for filing a NORS report but were never submitted.[19] Thereafter, Charter also identified two

[10] *Id*.

[11] *Id.*; *see also* Charter Outage of February 19, 2023 (NORS Final Report # ON-00438745). The affected states included portions of Alabama, Arizona, California, Colorado, Connecticut, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

[12] LOI Response at 8; *see also* Charter Outage of February 19, 2023 (NORS Final Report # ON-00438745).

[13] Dep't of Homeland Sec., Cybersecurity and Infrastructure Sec. Agency, "Understanding Denial of Service Attacks," https://www.cisa.gov/news-events/news/understanding-denial-service-attacks (last visited July 1, 2024).

[14] *See* Response to Second Further Letter of Inquiry, Counsel to Charter, Wilkinson Barker Knauer LLP, to Spectrum Enforcement Division, FCC Enforcement Bureau at 3-5, 9 (Nov. 13, 2023).

[15] 47 CFR § 4.9(g)(1)(i); LOI Response at 24; *see also* Response to Follow-Up Letter of Inquiry at 1-2, Counsel to Charter, Wilkinson Barker Knauer LLP, to Spectrum Enforcement Division, FCC Enforcement Bureau (Sept. 27, 2023) (Follow-Up LOI Response) (on file in EB-SED-23-00035290).

[16] *See* Letter of Inquiry from Spectrum Enforcement Division, FCC Enforcement Bureau, to Charter Communications, Inc. (June 1, 2023) (LOI); E-mail from Spectrum Enforcement Division, FCC Enforcement Bureau, to Counsel for Charter Communications, Inc. (Sept. 13, 2023, 14:24 EDT); E-mail from Spectrum Enforcement Division, FCC Enforcement Bureau, to Counsel for Charter Communications, Inc. (Oct. 19, 2023, 10:35 EDT); E-mail from Spectrum Enforcement Division, FCC Enforcement Bureau, to Counsel for Charter Communications, Inc. (Jan. 19, 2024, 15:01 EDT) (Disclosure Follow-up Email) (all on file in EB-SED-23-00035290).

[17] *See supra* notes 9 and 14; *see also* Response to Second Follow-Up Letter of Inquiry, Counsel to Charter, to Spectrum Enforcement Division, FCC Enforcement Bureau (Nov. 13, 2023) (all on file in EB-SED-23-00035290).

[18] LOI, *supra* note 16, at 10.

[19] Follow-Up LOI Response, *supra* note 15, at 4.

additional, unplanned outages—which occurred on March 31, 2023, and April 26, 2023—that each met the NORS reporting threshold but Charter failed to report.[20]

9. The Company and the Bureau subsequently engaged in settlement negotiations. To resolve this matter, the Company and the Bureau enter into this Consent Decree and agree to the following terms and conditions.

III. TERMS OF AGREEMENT

10. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order.

11. **Jurisdiction**. The Company agrees that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree.

12. **Effective Date; Violations**. The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

13. **Termination of Investigation**. In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigation. In consideration for the termination of the Investigation, the Company agrees to the terms, conditions, and procedures contained herein. The Bureau further agrees that, in the absence of new material evidence, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute any new proceeding on its own motion against the Company concerning the matters that were the subject of the Investigation, or to set for hearing the question of the Company's basic qualifications to be a Commission licensee or hold Commission licenses or authorizations based on the matters that were the subject of the Investigation.[21]

14. **Admission of Liability.** Charter admits for the purpose of this Consent Decree, for Commission civil enforcement purposes, and in express reliance on the provisions of paragraph 13 herein, that by its actions described in paragraphs 4 through 9 of this Consent Decree, Charter (i) failed to timely notify certain PSAPs of the Outage, (ii) failed to timely file NORS reports associated with the Outage, and the March 31, 2023 and April 26, 2023 outages, and (iii) failed to meet other NORS reporting deadlines associated with hundreds of unrelated planned maintenance outages, all in violation of the Notification Rules.

15. **Compliance Officer**. Within thirty (30) calendar days after the Effective Date, the Company shall designate a vice president or above with requisite corporate, budget, and organizational authority to serve as a Compliance Officer and to discharge the duties set forth below. The person designated as the Compliance Officer shall be responsible for overseeing the development, implementation, and administration of the Compliance Plan and ensuring that the Company complies with the terms and conditions of the Compliance Plan and this Consent Decree. In addition to the general knowledge of the Communications Laws necessary to discharge his or her duties under this Consent Decree, the Compliance Officer shall have specific knowledge of the 911 Rules prior to assuming his/her duties. The Compliance Officer must report in writing at least every six months to Charter's Chief Executive Officer on Charter's efforts during the relevant period to comply with the terms and conditions of this Consent Decree.

16. **Compliance Plan**. For purposes of settling the matters set forth herein, Charter agrees that it shall, within the dates set out below, develop and implement a Compliance Plan designed to ensure

[20] *See* Response to Disclosure Follow-up Email, Counsel to Charter, to Spectrum Enforcement Division, FCC Enforcement Bureau (Jan. 26, 2024) (on file in EB-SED-23-00035290).

[21] *See* 47 CFR § 1.93(b).

future compliance with the 911 Rules and the terms and conditions of this Consent Decree. By the dates set forth below, and continuing until the Termination Date of this Consent Decree, Charter shall develop and implement, or, where processes already exist, improve upon, processes related to the 911 Rules promptly to (1) *Govern* the Company's risk management strategies, expectations, and policies to identify, protect against, detect, respond to, and recover from outages; (2) *Identify* risks that could result in outages; (3) *Protect* against such risks; (4) *Detect* outages when they occur; (5) *Respond* to such outages with remedial actions; and (6) *Recover* from such outages as soon as practicable. With respect to the 911 Rules, Charter will implement, at a minimum, the following procedures:

(a) **Operating Procedures**. Within thirty (30) calendar days after the Effective Date, Charter shall establish Operating Procedures that all Covered Employees shall follow to help ensure that Charter complies with the 911 Rules. The Operating Procedures shall include, but are not limited to, the following:

i. **Develop Compliance Checklist.** Charter shall develop a compliance checklist that describes the steps for Charter to follow to comply with the 911 Rules.

ii. **Review and Improve PSAP Notification Procedures.** Charter shall establish and implement Operating Procedures (including, as necessary, reviewing and revising any existing procedures) to ensure that Charter has the ability promptly to identify PSAPs potentially impacted by a network outage and to notify such PSAPs, as required under section 4.9 of the Commission's Rules. Specifically, Charter will develop within sixty (60) days and implement within one-hundred and twenty (120) calendar days after the Effective Date, an automated PSAP notification system to automatically contact PSAPs after a network outage that meets the reporting thresholds in the 911 Rules. In developing and implementing this system, Charter shall without limitation:

1. Implement a monitoring system that checks the status of Charter's network to identify potential outages or disruptions in service.
2. Maintain an updated database of contact information for relevant PSAPs, including points of contact, phone numbers, emails, and any special requirements for reporting network outages.
3. Develop an automated protocol to initiate contact with potentially affected PSAPs in case of a network outage.
4. Ensure the automated PSAP notification system can provide the information set forth in the *PSAP Notification Order*.[22] In addition, ensure compliance with 47 C.F.R. § 4.9(h)(2) at the time those rules become effective.[23]
5. Ensure that the automated PSAP notification system has a confirmation mechanism that allows Charter to verify delivery.
6. Conduct quarterly testing of the automated PSAP notification system to ensure the system's functionality and that notifications are being timely sent.

Additionally, beginning on the first anniversary of the Effective Date and

[22] *See Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications, Improving 911 Reliability, New Part 4 of the Commission's Rules Concerning Disruptions to Communications,* PS Docket Nos. 15-80, 13-75, 04-35, Second Report and Order, FCC 22-88 at 6, para. 14 (Nov. 18, 2022) (*PSAP Notification Order*).

[23] The effective date of 4.9(h) has been delayed until announcement in the Federal Register. Federal Communications Commission, Disruptions to Communications; Improving 911 Reliability, Final Rule, 88 Fed. Reg. 9756 (Feb. 15, 2023). The compliance requirement remains if this provision becomes effective and is codified in a different subsection of section 4.9 of the Rules.

continuing annually until the Termination Date of this Consent Decree, Charter shall: (a) review its PSAP notification procedures to identify modifications that could reduce the time needed to identify and notify potentially impacted PSAPs; and (b) within thirty (30) days of such review, implement any such modifications as are economically feasible. If Charter is unable to implement such modification within thirty (30) days, Charter shall complete implementation within a reasonable amount of time and notify the Commission within the thirty (30) day time-period of details on the nature of the modification and a timeline for implementation.

iii. **Review and Implement Best Practices**. Within ninety (90) calendar days of the release by the Communications Security, Reliability, and Interoperability Council (CSRIC) of any new and applicable best practices relating to 911 service, Charter shall evaluate and incorporate, where appropriate, such new best practices into the Operating Procedures and shall establish a timeline for their implementation following the release of such new and applicable best practices. Additionally, within ninety (90) days after the Effective Date, Charter shall evaluate and incorporate, where appropriate, the CSRIC Best Practices set forth in Appendix A. If implementation of any of the best practices under this paragraph shall exceed one hundred and eighty (180) days, Charter shall notify the Commission, specifying the applicable best practice and Charter's implementation timeline.

iv. **Perform 911 Operational Risk Assessments**. Charter shall maintain, regularly review, and revise (as necessary) a risk-assessment program designed to identify, assess, and remediate risks to Charter's ability to transmit 911 calls, including third-party or vendor risks. Charter shall also identify the primary risks to Charter's 911 transmission and delivery network and implement risk and management controls and methodologies to address those risks, with specific attention to those issues that were identified as the root cause of the Outage and other contributing factors underlying the root cause. Charter shall utilize an industry-recognized risk control methodology that provides, at a minimum, that:

1. Charter shall develop key risk indicators for compliance with the 911 Rules.
2. Charter shall assess, at least annually, internal and external risks to the security, integrity, and resiliency of Charter's network and its ability to transmit 911 calls consistent with the 911 Rules.
3. Charter shall assess and test, at least annually, the sufficiency and effectiveness of any safeguards in place in paragraph 16(a)(iv)(2) to address the identified risks and timely modify such safeguards, as appropriate.
4. Prior to approving any new software, hardware or systems that impact Charter's ability to transmit 911 calls, Charter shall perform a risk analysis of Charter's network and its ability to transmit 911 calls. Where feasible, Charter shall employ appropriate controls to address risk prior to installing such new software, hardware or systems that could impact Charter's ability to transmit 911 calls.

v. **Create and Maintain NORS Evaluation and Reporting System.** Develop within thirty (30) calendar days and implement within sixty (60) calendar days after the Effective Date, a system to automatically determine when a NORS report needs to be filed because of a network outage that meets the reporting thresholds in the 911 Rules. The system shall include, but not be limited to:

1. Create and improve upon network outage report tracking tools to, at a minimum:

a. monitor in real-time network outages to identify the scope, severity, and duration of the outage;

b. establish internal protocols and workflows for handling outage analysis and reporting, including developing reporting that can correlate assigned or working telephone numbers to a voice circuit or service to determine whether NORS reporting thresholds have been met;

c. implement checks and balances to verify the accuracy and completeness of the outage data before submission of the final report to the NORS;

d. incorporate processes for notifications, escalations, and reminders to notify the Compliance Officer of missed reporting deadlines; and

e. review and refine network outage reporting processes based on incident analysis and feedback from Covered Employees on at least a monthly basis in order to enhance compliance with the 911 Rules.

2. Within thirty (30) calendar days after the Effective Date, the Compliance Officer shall designate a Covered Employee to review, on a monthly basis, network outage data associated with Charter outages to verify that, for outages that meet the NORS reporting thresholds, Charter has timely filed, as applicable, all required Notifications, Initial Reports, and/or Final Reports for all reportable network outages. The designated Covered Employee shall report the results of these reviews to the Compliance Officer.

vi. **Cybersecurity**. Charter has established and shall continue to maintain and evolve its overall cybersecurity risk management program in accordance with the voluntary cybersecurity framework established by the NIST[24] through the NIST Cyber Security Framework, other applicable industry standards and best practices, and applicable state and/or federal laws covering cybersecurity risk management and governance practices, including the following:

1. *Vulnerability Identification.* Charter shall maintain an active vulnerability management program to scan its environment for vulnerabilities consistent with the NIST Cybersecurity Framework. Charter shall maintain its active threat management effort, as appropriate.

2. *Penetration Testing.* Charter shall maintain a penetration testing program that regularly tests, based on risk profile and criticality, its systems, applications, and network infrastructure for the purpose of identifying technical weaknesses that a malicious user could exploit. The program shall leverage tools and techniques a threat actor would utilize to demonstrate risks to Charter systems.

3. *Vulnerability Mitigation*. Charter shall maintain internal policies and practices to mitigate vulnerabilities in a risk-based prioritized manner, including to rate and rank the severity of all vulnerabilities revealed as a result of scanning, vendor notifications, publication in CISA's Known Exploited Vulnerabilities catalog, and penetration testing, and take such actions as are necessary to mitigate any vulnerability that threatens Charter's ability to transmit 911 calls as soon as possible.

[24] Nat'l Inst. of Standards and Tech., February 2024 Cybersecurity Framework Version 2.0, https://www.nist.gov/cyberframework (last visited July 1, 2024).

4. *Vendor Management*. Charter shall maintain policies and practices to regularly review and assess vendor risk and, where appropriate, consider clauses in future contracts that require vendors and service providers to: (a) proactively identify and disclose to Charter confirmed security vulnerabilities applicable to Charter; (b) promptly notify Charter of such confirmed security vulnerabilities; (c) communicate details about the vulnerability, its potential impact, and any recommended mitigation strategies; and (d) complete industry standard audits like System and Organization Control (SOC) 2 assessments.

5. *Network Segmentation*. Charter shall maintain, as practicable, policies and procedures to implement a "deny-by-default" standard for operational technology network connections, requiring explicit whitelisting with Internet protocol and port restrictions. The policies and procedures shall require that all necessary operational technology communications must traverse monitored and logged intermediary controls (e.g., firewalls, bastions, etc.), shall allow only approved asset connections, and shall minimize the risk of attacker access, even if the network is breached.

6. *Manage Internet-Facing Services*. Charter shall maintain, as practicable, an operational technology security set of standards and procedures intended to minimize public Internet exposure and mandating additional protections (e.g., logging, multi-factor authentication, secure access) for justified exceptions, to mitigate threat actor exploitation and interruption risks. The standards and procedures shall include principles that eliminate, as practicable, exploitable services; control necessary exceptions; and disable all unnecessary operating system applications and network protocols on Internet-facing assets.

vii. **Cybersecurity Incident Reporting.** Consistent with its current practices and in accordance with applicable laws and regulations, Charter shall review and update within sixty (60) days of the Effective Date clear and actionable policies and procedures, including to whom and how submissions are made, to provide timely cyber incident reporting to CISA and other Sector Risk Management Agencies (SRMA).[25] Once Charter has developed or updated such cybersecurity incident reporting policies, Charter shall notify CISA of confirmed cybersecurity incidents consistent with applicable laws and regulations governing incident reporting. In addition, Charter shall promptly notify the relevant SRMA, as determined by the nature of the incident and its potential impact.

(b) **Compliance Manual**. Within sixty (60) calendar days after the Effective Date, the Compliance Officer shall develop and distribute a Compliance Manual to all Covered Employees. The Compliance Manual shall explain the 911 Rules and set forth the Operating Procedures that Covered Employees shall follow to help ensure the Company's compliance with the 911 Rules and to implement the Operating Procedures. The Company shall periodically review and revise the Compliance Manual as necessary to ensure that the information set forth therein remains current and accurate. The Company shall distribute any revisions to the Compliance Manual promptly to all Covered Employees.

[25] SRMAs are government-led entities that focus on special critical infrastructure sectors and help those sectors identify, assess, and mitigate risks related to cyber threats, physical threats, and other vulnerabilities.

(c) **Compliance Training Program**. The Company shall establish and implement a Compliance Training Program on compliance with the 911 Rules and Operating Procedures. Charter's Compliance Training Program shall address, at a minimum: (i) the methods, procedures, and calculations used to identify reportable network outages; (ii) the time periods within which applicable Notifications, Initial Reports, and Final Reports must be filed with the Commission; and (iii) the potential regulatory and internal disciplinary consequences of failing to comply with the 911 Rules and Charter's Operating Procedures. As part of the Compliance Training Program, Covered Employees shall be advised of the Company's obligation to report any noncompliance with the 911 Rules under paragraph 17 of this Consent Decree and shall be instructed on how to disclose noncompliance to the Compliance Officer. All Covered Employees shall be trained pursuant to the Compliance Training Program within ninety (90) calendar days after the Effective Date, except that any person who becomes a Covered Employee at any time after the initial Compliance Training Program shall be trained within thirty (30) calendar days after the date such person becomes a Covered Employee. The Company shall repeat compliance training on an annual basis, and shall periodically review and revise the Compliance Training Program as necessary to ensure that it remains current and complete and to enhance its effectiveness.

17. **Reporting Noncompliance**. The Company shall report any noncompliance with the 911 Rules and with the terms and conditions of this Consent Decree within fifteen (15) calendar days after discovery of such noncompliance. If additional investigation is required by Charter, Charter may provide an updated noncompliance report within fifteen (15) calendar days after the initial report of material noncompliance. Such reports shall include a detailed explanation of: (i) each instance of such noncompliance, including the geographic area affected and the impact, if any, on 911 call transmission, NORS reporting and PSAP notification; (ii) the steps that the Company has taken or will take to remedy such noncompliance; (iii) the schedule on which such remedial actions will be taken; and (iv) the steps that the Company has taken or will take to prevent the recurrence of any such noncompliance. Such noncompliance reports shall include an affidavit or declaration consistent with section 1.16 of the Commission's Rules and be subject to the accuracy requirements of section 1.17 of the Commission's Rules.[26] All reports of noncompliance shall be submitted electronically to Chief, Spectrum Enforcement Division, Enforcement Bureau, Federal Communications Commission, via EB-SED-Response@fcc.gov. Each report of noncompliance filed pursuant to this paragraph 17 shall be provided to the Compliance Officer.

18. **Compliance Reports**. The Company shall file compliance reports with the Commission ninety (90) calendar days after the Effective Date, twelve (12) months after the Effective Date, twenty-four (24) months after the Effective Date, and thirty-six (36) months after the Effective Date.

(a) Each Compliance Report shall include a detailed description of the Company's efforts during the relevant period to comply with the terms and conditions of this Consent Decree and the 911 Rules. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of the Company, stating that the Compliance Officer: (i) has personal knowledge that the Company: (a) has established and implemented the Compliance Plan; and (b) has utilized the Operating Procedures since the implementation of the Compliance Plan; and (ii) is not aware of any instances of noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in paragraph 17 of this Consent Decree.

[26] 47 CFR § 1.16.

(b) The Compliance Officer's certification shall be accompanied by a statement explaining the basis for such certification and shall comply with section 1.16 of the Rules and be subscribed to as true under penalty of perjury in substantially the form set forth therein.[27]

(c) If the Compliance Officer cannot provide the requisite certification, then the Compliance Officer, as an agent of and on behalf of the Company, shall instead provide the following:

i. For any instance of noncompliance that the Company has not previously reported to the FCC under paragraph 17: (1) a detailed description of the noncompliance; (2) the steps that the Company has taken or will take to remedy such noncompliance, including the schedule on which proposed remedial actions will be taken; and (3) the steps that the Company has taken or will take to prevent the recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

ii. For any instance of noncompliance that the Company has previously reported pursuant to paragraph 17, the Compliance Officer will include with the Compliance Report: (1) copies of those reports and (2) any material new information about the instance of noncompliance that the Company has obtained since the filing of the report; (3) the steps that the Company has taken or will take to remedy such noncompliance, including the schedule on which proposed remedial actions will be taken; and (4) the steps that the Company has taken or will take to prevent the recurrence of any such noncompliance, including the schedule on which such preventive action will be taken.

(d) All Compliance Reports shall be submitted electronically to Chief, Spectrum Enforcement Division, Enforcement Bureau, Federal Communications Commission, via EB-SED-Response@fcc.gov.

19. **Termination Date**. Unless stated otherwise, the requirements set forth in paragraphs 15 through 18 of this Consent Decree shall expire thirty-six (36) months after the Effective Date.

20. **Civil Penalty**. The Company will pay a Civil Penalty to the United States Treasury in the amount of fifteen million dollars ($15,000,000) in accordance with the following terms. Such payments shall be made in four (4) installments (each an Installment Payment). The first installment payment in the amount of three million seven hundred and fifty thousand dollars ($3,750,000) is due within thirty (30) calendar days of the Effective Date. Thereafter, subsequent Installment Payments of three million seven hundred and fifty thousand dollars ($3,750,000) will be due every ninety (90) days thereafter for the next two hundred seventy (270) days. The Company acknowledges and agrees that upon execution of this Consent Decree, the Civil Penalty and each Installment Payment shall become a "Claim" or "Debt" as defined in 31 U.S.C. § 3701(b)(1).[28] Upon an Event of Default, all procedures for collection as permitted by law may, at the Commission's discretion, be initiated. The Company shall send electronic notification of payment to EB-SED-Response@fcc.gov on the dates that payments are made. Payment of the Civil Penalty must be made by credit card using the Commission's Registration System (CORES) at https://apps.fcc.gov/cores/userLogin.do, ACH (Automated Clearing House) debit from a bank account, or by wire transfer from a bank account. The Commission no longer accepts Civil

[27] *Id*.

[28] Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, 110 Stat. 1321, 1358 (Apr. 26, 1996).

Penalty payments by check or money order. Below are instructions that payors should follow based on the form of payment selected:[29]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. In the OBI field, enter the FRN(s) captioned above and the letters "FORF". In addition, a completed Form 159[30] or printed CORES form[31] must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 or CORES may result in payment not being recognized as having been received. When completing FCC Form 159 or CORES, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[32] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the CD Acct. No. The bill number is the CD Acct. No. with the first two digits excluded (e.g., CD 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the CD Acct. No. The bill number is the CD Acct. No. with the first two digits excluded (e.g., CD 1912345678 would be associated with FCC Bill Number 12345678). Finally, choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

21. **Event of Default**. The Company agrees that an Event of Default shall occur upon the failure by the Company to pay the full amount of the Civil Penalty or any Installment Payment on or before the due date specified in this Consent Decree.

22. **Interest, Charges for Collection, and Acceleration of Maturity Date**. After an Event of Default has occurred under this Consent Decree, the then unpaid amount of the Civil Penalty or any Installment Payment shall accrue interest, computed using the U.S. Prime Rate in effect on the date of the Event of Default plus 4.75%, from the date of the Event of Default until payment in full. Upon an Event

[29] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6), or by e-mail at ARINQUIRIES@fcc.gov.

[30] FCC Form 159 is accessible at https://www.fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159.

[31] Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form 159. CORES is accessible at https://apps.fcc.gov/cores/userLogin.do.

[32] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

of Default, the then unpaid amount of the Civil Penalty or any Installment Payment, together with interest, any penalties permitted and/or required by the law, including but not limited to 31 U.S.C. § 3717, and administrative charges, plus the costs of collection, litigation, and attorneys' fees, shall become immediately due and payable, without notice, presentment, demand, protest, or notice of protest of any kind, all of which are waived by the Company.

23. **Waivers**. As of the Effective Date, the Company waives any and all rights it may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this Consent Decree and the Adopting Order. The Company shall retain the right to challenge Commission interpretation of the Consent Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the Consent Decree or the Adopting Order, neither the Company nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and the Company shall waive any statutory right to a trial *de novo*. The Company hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act[33] relating to the matters addressed in this Consent Decree.

24. **Severability**. The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

25. **Invalidity**. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

26. **Subsequent Rule or Order**. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or order adopted by the Commission (except an order specifically intended to revise the terms of this Consent Decree to which the Company does not expressly consent) that provision will be superseded by such Rule or order.

27. **Successors and Assigns**. The Company agrees that the provisions of this Consent Decree shall be binding on its successors, assigns, and transferees.

28. **Final Settlement**. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigation.

29. **Modifications**. This Consent Decree cannot be modified without the advance written consent of both Parties.

30. **Paragraph Headings**. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

31. **Authorized Representative**. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

[33] *See* 5 U.S.C. § 504; 47 CFR §§ 1.1501-1.1530.

32. **Counterparts**. This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

_____
Loyaan A. Egal
Chief
Enforcement Bureau

_____
Date

_____
Clifford S. Harris
Senior Vice President – Legal, Programming, Product & Regulatory
Charter Communications, Inc.

_____
Date

APPENDIX A
Applicable CSRIC Best Practices

CSRIC Best Practice	Description
13-8-8090	Network Operators, Service Providers, and Equipment Suppliers should restrict dynamic port allocation protocols such as Remote Procedure Calls (RPC) and some classes of Voice-over-IP protocols (among others) from usage, especially on mission critical assets, to prevent host vulnerabilities to code execution. Dynamic port allocation protocols should not be exposed to the Internet. If used, such protocols should be protected via a dynamic port knowledgeable filtering firewall or other similar network protection methodology.
13-8-8664	Network Operators and Service Providers should block protocols meant for internal VoIP call control use at the VoIP perimeter.
13-12-8022	Network Operators, Service Providers and Public Safety should have a process by which there is a risk assessment and formal approval for all external connections. All such connections should be individually identified and restricted by controls such as strong authentication, firewalls, limited methods of connection, and fine-grained access controls (e.g., granting access to only specified parts of an application). The remote party's access should be governed by contractual controls that ensure the provider's right to monitor access, defines appropriate use of the access, and calls for adherence to best practices by the remote party. This applies to Public Safety only in an NG9-1-1 environment.
13-7-8077	Network Operators, Service Providers should use access control lists (ACLs) to restrict which machines can access the device and/or application if they do not have adequate access control capabilities. This applies to legacy systems. In order to provide granular authentication, a bastion host that logs user activities should be used to centralize access to such devices and applications, where feasible.
13-12-3275	Network Operators, Service Providers, Equipment Suppliers and Public Safety should support Border Control Functions (BCFs) that provide border firewall functionality including application and network layer protection and scanning, resource and admission control, and Denial of Service (DoS) detection and protection, as well as Session Border Control (SBC) functionality including: identification of emergency call/session and priority handling for the IP flows of emergency call/session traffic; conformance checking and mapping (if applicable) of priority marking based on policy for emergency calls/sessions; SIP protocol normalization; Network Address Translation (NAT) and Network Address and Port Translation (NAPT) Traversal; IPv4/IPv6 Interworking; Signaling Transport Protocol Support; and QoS/Priority Packet Marking.