Description of document:	Federal Communications Commission (FCC) Standard Operating Procedure (SOP) for Network Outage Reporting System (NORS) 2023
Requested date:	2023
Release date:	05-May-2023
Posted date:	24-June-2024
Source of document:	Freedom of Information Act Request Federal Communications Commission 45 L Street NE Washington, D.C. 20554 ArkCase FOIA

Federal Communications Commission
Washington, D.C. 20554

May 5, 2023

VIA ELECTRONIC MAIL

Re: FOIA Control No. 2023-000437

This letter responds to your Freedom of Information Act (FOIA) request for "FCC Standard Operating Procedure (SOP) for Incident Response."[1] Your request has been assigned FOIA Control No. 2023-000437.

Pursuant to section 0.461(g)(1)(iii) of the Commission's rules, the date for responding to your request has been extended from April 19, 2023, to May 3, 2023, due to a need to search records from multiple offices of the Commission. In the courses of our search, we determined that it was necessary to request clarification of the term "incident response." We notified you of the request on April 18, 2023 and tolled the deadline for responding to your request pursuant to section 0.462(e)(2)(i)(A) of the Commission's rules.[2] In response to our request for clarification, you stated, "I agree to limit the search to those documents have already been located and retrieved. I do not request any further search."[3]

The Public Safety and Homeland Security Bureau, Operations and Emergency Management Division searched for responsive records. We located 11 pages of records responsive to your request. Some material on the pages produced has been redacted due to the reasons discussed below.

Records responsive to your request were redacted under FOIA Exemption 6.[4] Exemption 6 protects "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Consistent with this standard, and balancing the public's right to disclosure against the individual's right to privacy, we have determined that it is reasonably foreseeable that disclosure of their personal information, including names, phone numbers, and email addresses, would harm the privacy interests of the persons mentioned in these records, which

[1] FOIA Control No. 2023-000437 (submitted Mar. 22, 2023).

[2] Email from John Adams, Attorney Advisor, Federal Communications Commission, to Michael Ravnitzky (Apr. 18, 2023, 17:10 EDT).

[3] Email from Michael Ravnitzky to John Adams, Attorney Advisor, Federal Communications Commission (Apr. 18, 2023, 18:19 EDT).

[4] 5 U.S.C. § 552(b)(6).

Exemption 6 is intended to protect. Additionally, the FCC employees named in the documents are involved in sensitive operational matters and thus may be more likely to face possible harassment if their personal information were to be disclosed under the FOIA.

Records responsive to your request were also redacted under Exemption 7(E), which protects "records or information compiled for law enforcement purposes [the production of which] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk a circumvention of the law."[5] The redacted information consists of operational tactics, procedures, and infrastructure. We have determined that it is reasonably foreseeable that disclosure of this information would harm the Commission or the Federal government's law enforcement and incident management activities, which Exemption 7 is intended to protect.

The FOIA requires that "any reasonably segregable portion of a record" must be released after appropriate application of the Act's exemptions.[6] The statutory standard requires the release of any portion of a record that is nonexempt and that is "reasonably segregable" from the exempt portion. However, when nonexempt information is "inextricably intertwined" with exempt information, reasonable segregation is not possible.[7] The redactions made are consistent with our responsibility to determine if any segregable portions can be released. To the extent non-exempt material is not released, it is inextricably intertwined with exempt material.

We also reviewed the redacted records to determine if discretionary release is appropriate.[8] The materials that are protected from disclosure under Exemption 6 are not appropriate for discretionary release in light of the personal privacy interests involved. The materials that are protected from disclosure under Exemption 7 are not appropriate for discretionary release in light of the law enforcement and operational sensitivities involved.

We are required by both the FOIA and the Commission's own rules to charge requesters certain fees associated with the costs of searching for, reviewing, and duplicating the sought after information.[9] To calculate the appropriate fee, requesters are classified as: (1) commercial use requesters; (2) educational requesters, non-commercial scientific organizations, or representatives of the news media; or (3) all other requesters.[10]

---

[5] 5 U.S.C. § 552(b)(7)(E).

[6] 5 U.S.C. § 552(b) (sentence immediately following exemptions).

[7] *Mead Data Cent. Inc. v. Dep't of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977).

[8] *See* President's Memorandum for the Heads of Executive Departments and Agencies, Freedom of Information Act, 74 Fed. Reg. 4683 (2009).

[9] *See* 5 U.S.C. § 552(a)(4)(A); 47 CFR § 0.470.

[10] 47 CFR § 0.470.

Pursuant to section 0.466(a)(8) of the Commission's rules, you have been classified for fee purposes under category (3) as an "all other requester."[11] As an "all other requester," the Commission assesses charges to recover the full, reasonable direct cost of searching for and reproducing records that are responsive to the request; however, you are entitled to be furnished with the first 100 pages of reproduction and the first two hours of search time without charge under section 0.470(a)(3)(i) of the Commission's rules.[12] The production in response to your request required less than two hours of search time, and was provided in electronic form. Therefore, you will not be charged any fees.
If you consider this to be a denial of your FOIA request, you may seek review by filing an application for review with the Office of General Counsel. An application for review must be *received* by the Commission within 90 calendar days of the date of this letter.[13] You may file an application for review by mailing the application to Federal Communications Commission, Office of General Counsel, 45 L Street NE, Washington, DC 20554, or you may file your application for review electronically by e-mailing it to FOIA-Appeal@fcc.gov. Please caption the envelope (or subject line, if via e-mail) and the application itself as "Review of Freedom of Information Action."

If you would like to discuss this response before filing an application for review to attempt to resolve your dispute without going through the appeals process, you may contact the Commission's FOIA Public Liaison for assistance at:

FOIA Public Liaison
Federal Communications Commission
Office of the Managing Director
Performance Evaluation and Records Management
45 L Street NE, Washington, DC 20554
202-418-0440
FOIA-Public-Liaison@fcc.gov

If you are unable to resolve your FOIA dispute through the Commission's FOIA Public Liaison, the Office of Government Information Services (OGIS), the Federal FOIA Ombudsman's office, offers mediation services to help resolve disputes between FOIA requesters and Federal agencies. The contact information for OGIS is:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road–OGIS
College Park, MD 20740-6001
202-741-5770
877-684-6448
ogis@nara.gov
https://www.archives.gov/ogis

---

[11] 47 CFR § 0.466(a)(8).

[12] 47 CFR § 0.470(a)(3)(i).

[13] 47 CFR §§ 0.461(j), 1.115; 47 CFR § 1.7 (documents are considered filed with the Commission upon their receipt at the location designated by the Commission).

Sincerely,

JUSTIN CAIN Digitally signed by JUSTIN CAIN
Date: 2023.05.05 17:11:23
-04'00'

Justin N. Cain
Chief, Operations and Emergency Management Division
Public Safety and Homeland Security Bureau

cc: FCC FOIA Office

STANDARD OPERATING PROEDURES (SOP) NR: 01
NETWORK OUTAGE REPORTING SYSTEM (NORS)

Originated on: 07/15/05

Revised by: FS 2/13/2023 Annual review due: 01/2024

Purpose: To establish procedures for handling email notifications of network and 911 outages reported through the Network Outage Reporting System (NORS) in the FCC Operations Center (FCCOC).
Introduction: The FCC requires communications providers, including wireline, wireless, paging, cable satellite and Signaling System 7 service providers to electronically report information about significant disruptions/outages to their systems that meet specified thresholds set forth in the FCC's 47 CFR Part 4 rules. Communications providers must also report information regarding communications disruptions affecting enhanced 9-1-1 facilities and airports that meet the thresholds set forth in Part 4 of the FCC's rules. NORS automatically sends e-mail alerts to the Department of Homeland Security (DHS), the FCCOC, and designated members within PSHSB when a network or 911 outage has exceeded an established threshold. On a 24-hour basis, the FCCOC monitors these reports to determine if the disruption or outage may have an effect on public safety/homeland security-related emergency networks. *The FCCOC also monitors a NORS dashboard for real-time outages looking for trends that could be of concern should*

*******Due to proprietary reasons NORS data and contact information CANNOT be released outside the FCC without CCR consult*******

Email reporting "Outage Report – Threshold is crossed"

1. Access the outage report directly by clicking on the hyperlink on the bottom of the email.
   a. If you are having issues logging in directly go through (b) (7)(E) and click on Service Now
2. Review the information in the detailed report to determine the severity of the outage.
   a. Originates from malicious or accidental activity.
   b. Is it affecting multiple locations, outage ongoing or resolved?

	CATASTROPHIC	MAJOR
Wireline User Minutes	**>2,000,000**	**>150,000**
Wireless (non-paging) User Minutes	**>2,000,000**	**>150,000**
Cable Telephone User Minutes	**>2,000,000**	**>150,000**
Blocked Calls	**>2,000,000**	**>450,000**
VoIP	**>2,000,000**	**>150,000**
OC3's	**Monitor above major**	**>10,000**

3. If the outage is considered **MAJOR** or the report contains updates that the issue is resolved: Email NORS Team with all the pertinent information; verbal contact not required.

4. If the outage is considered **CATASTROPHIC** or the detailed information needs to be verified: Contact the NORS Team **via telephone and email regardless of the time of day**
   a. If contact **cannot be established** with a NORS Team member within 30 minutes contact the carrier POC on NORS report for status
   a. If contact **cannot be established** with the company within 30 minutes contact the PSHSB/CCR Division Chiefs; they will escalate and follow up with FCCOC.
   b. If the outage is verified Catastrophic and is ongoing, initiate SOP 19 Emergency Information Dissemination Distribution List C and relay all updates as received

Email reporting: "911 Outage Received" (E911 Notification Report)

1. Review the '**E911 Outage – Location Affects**' field to determine what services are affected

Code	Term	Definition
Blank	E911 Not Affected	Non-E911 outages
1	ALI Only Affected	for wireline carriers when location of the caller could not be provided, but the call could be routed to a public-safety answering point (PSAP).
2	Phase II Only Affected	for wireless outages when Phase II location information could not be provided, but the call could be routed to a PSAP.
3	Phase I and Phase II Only Affected	for wireless outages when neither Phase I nor Phase II could be provided, but the call could be routed to a PSAP
4	More than Location Affected	for wireline and wireless carriers when the call could NOT be routed to the appropriate PSAP

2. Review the '**Description of Incident**' field to determine the severity of the outage and contact the Public Safety Answering Point (PSAP) using the latest PSAP Listing if:
   a. The extent and/or status of the outage cannot be determined
   b. The outage prevents the PSAP from receiving calls and calls are **NOT** being rerouted to Admin Lines or alternate PSAP
   c. The report mentions PSAP Isolation, OOS (Out of Service), disruption, etc.

3. PSAP contact and reporting:
   a. Call PSAP using the latest PSAP listing to determine status- (b) (7)(E) [redacted]
   b. If unable to reach PSAP directly- call a neighboring PSAP(s) to see if they are receiving impacted PSAP calls, if they have a status, or an alternate "inside" number to PSAP
   c. If unable to ascertain PSAP status- call NORS team for assistance
      i. If unable to reach NORS team verbally and no call back after 30 minutes, contact carrier POC on NORS report for status
      ii. Send email to NORS team with carries PSAP status
   d. If PSAP requests FCC assistance, verbally notify NORS team per calling list below
   e. If PSAP reports the outage is restored, or they have a workaround in place, or no assistance is required, notify NORS team via email that status was verified, and no further action is required

Email reporting: "FCC NORS Notification of Cyber Event Received."

1. Review the event in NORS
2. During normal duty hours, **REPLY ALL and add**:
   (Subject: FCCOC in receipt of NORS Cyber Event Report)
   a. (b) (6) [redacted]
   b. (b) (6) [redacted]
   c. (b) (6) [redacted]
   d. (b) (6) [redacted]

3. If after normal duty hours notify Michael Caiafa via phone, **REPLY ALL and add**:
   (Subject: FCCOC in receipt of NORS Cyber Event Report)
   In message body- (b) (6) has been verbally notified or FCCOC was unable to verbally reach (b) (6)
   a. (b) (6)
   b. (b) (6)
   c. (b) (6)
   d. (b) (6)

NORS Team "in order" for after-hours support (PSHSB/CCR)

NAME	OFFICE	FCC CELL	PERSONAL CELL	HOME
(b) (6)				

Due to proprietary reasons NORS data and contact information CANNOT be released outside the FCC without CCR consult

4. Email notifications to CCR:
   a. Any email correspondence to the NORS Team regarding NORS alerts that are listed in the Daily Brief as "CCR notified" must include the CCR Chief and Deputy.
      i. (b) (6)
5. **NORS Network Outage**
   a. If the NORS network goes down (providers are unable to file), notify:
      i. (b) (6)

STANDARD OPERATING PROCEDURES (SOP) NR: 19

EMERGENCY INFORMATION DISSEMINATION PROCEDURES

Date Created: 3/21/2008

Revised by: (b) (6) - 7/6/2020 Annual review due: 05/2023

Purpose: To establish procedures for Watch Officers to disseminate emergency information related to significant or catastrophic events

1. Responsibilities: The FCC Operations Center (FCCOC) has the responsibility to disseminate information related to significant or catastrophic events. This includes media reports, phone calls, NORS, or other sources. PSHSB Management has responsibility to act in response to significant or catastrophic events and will activate an Incident Management Team deemed appropriate by the FCC/PSHSB management based on the information provided.

2. Timing of Reports: In reporting such incidents to FCC management, time is of the essence. When emergency incident information is received, assessments of its validity and significance should be made as soon as possible. Briefly check for other reports/sources or call a relevant source for possible confirmation; i.e. the NCC. If it is determined that a report should be given to FCC management, it should be done immediately. Even if the incoming information is unconfirmed from a media source or a single source, it is preferable to pass it to management rather than have an extended delay of reporting waiting for more complete verification. If there are questions regarding whether notification should be made to FCC management, immediately contact the next level(s) up in the chain of command to determine the appropriate action.

NOTE: Ensure email template SOURCE OF INFORMATION is marked (Confirmed/Unconfirmed) (Single/Multiple) _____.

3. Method of Notification: During normal business hours, email is the preferred method of notification. During other than normal business hours, telephone calls are the preferred method of notification. If an incident is judged to be significant, then telephone notification will be made in addition to email.

4. Acknowledgement of Receipt of Emergency Notifications: It is important to ensure that emergency notifications by the FCCOC are received by FCC management. To that end, the FCCOC emergency emails should include the phrase “please acknowledge receipt of email with reply”. Telephone messages left with third parties or on answering machines should request return calls to acknowledge receipt. When email notifications are made, the FCCOC should review the reply acknowledgements and determine, in consultation with FCCOC Director, whether the emergency notification must be followed to ensure key FCC managers are aware of the situation.

5. Follow-up: After sending the initial report, the FCCOC will continue to monitor sources and provide email updates to FCC management as significant updates occur.

6. Tracking: The FCCOC will log any updates to the situation and inquiries/responses from FCC management in the Daily Activities Log.

7. Major Significant Events: If one of the following events or any event of similar significance occurs, the FCCOC will report the event to FCC management specified in **Distribution List A**:

a. A significant adverse event that occurs (b) (7)(E) of the FCC HQ or field office
b. An emergency incident and/or evacuation at the White House
c. A significant attack on any federal facility
d. A terrorist attack in the U.S.
e. A catastrophic event in a major U.S. city or impacting U.S. interests

NOTE: This alert should be used with caution. Ensure you have the correct facts and that you are thorough in event description.

8. Threats to Federal Personnel and Facilities: If one of the following events or any event of similar significance occurs, the FCCOC will report the event via email to FCC management specified in **Distribution List B**:

a. a report of a suspicious package/activity or threat against a Federal Building in the National Capital Area (NCR) or field office
    i. If threat is to FCC headquarters notify Security Command Center (b) (7)(E)
    ii. If threat is to FCC personnel, notify FCC SSO (Special Security Officer)
b. an emergency incident and/or an evacuation at a Federal Building in the NCR (except as noted in 7c above)
c. a report of an occurrence that may adversely affect FCC personnel arriving or departing FCC HQ during a workday (e.g., closure of major highway or public transportation portal, major demonstration, impending blizzard or other violent storms)
d. Major virus or pandemic outbreaks

9. Minor Significant Events: If one of the following events or any event of similar significance occurs, the FCCOC will report the event via email to FCC management specified in **Distribution List C**:

a. any confirmed event that may adversely affect communications networks such as media reported regional or multi-state outages, multiple NORS alerts that collectively could be of concern, NORS Dashboard showing clusters or large outages, false EAS and/or WEA alerts or system failures; statewide power outages over 50k customers, Public Safety Power Shutoffs, or impacts to other public safety systems.
b. Provide cause of outages if known such as weather, fiber cut, planned maintenance, etc.
    i. Call the NCC to see if they have any information, check NORS, call the NORS team if you require assistance. *Bottom line- be vigilant, proactive, and do not ignore potential impacts to communications.*

10. Prepared Email Distribution Lists: The FCCOC Director or the Senior Watch Officer will direct the preparation of email groups for Distribution Lists A, B and C to verify these email groups remain up to date and readily available for Watch Officer use as needed.

11. Initial format for all reporting: Use appropriate Outlook email template to draft and send report. (b) (7)(E)

12. Following receipt of an Initial Incident Report, FCC and PSHSB management will determine whether to activate an Incident Management Team and the appropriate level of team management.

STANDARD OPERATING PROCEDURES (SOP) NR: 34
SIGNIFICANT EVENT OPERATIONS

Originated: 09/04/08

Revised by: (b) (6) - 9/12/2022 Annual review due: 09/2023

Purpose: To establish procedures for operations during significant events

Introduction: A significant event is defined as any event; man-made or resulting from natural disaster; that may produce communications outages or result in a Federal Government response. The FCC Operations Center (FCCOC) is the initial point of contact for all events and the on-duty Senior Watch Officer is responsible for proper reporting. This SOP will mainly be used while the Incident Management Team (IMT) is activated but could be used as a guide for lesser significant events.

Types of Reports

1. Initial Reporting (See SOP 19)

Upon the first indication of a significant event review SOP 19 to determine the appropriate level of distribution and FCCOC K Drive email template to use. Send out a preliminary email within 30 minutes of discovery of event.

2. Detailed Report

A detailed report, SITREP, will be created using Gathering Information below. If approved by OEM Leadership, this report should go out as soon as all the data is collected, and report completed. Times will vary due to details however the report should go out as soon as possible.

NCS Conference Bridges

Upon notification of an NCC conference bridge for an event that could have communications outages the watch officer must review their sources and reach out to possible effected public safety entities. A brief report of findings and what was accomplished must be provided to the FCC/DHS Liaison via email prior to the NCS conference bridge.

Information Gathering

1. Use open media sources to obtain basic information (who, what, when, where, etc.), depending on the event, i.e. weather, earthquake, etc. Some examples are:
   a. www.nws.noaa.gov
   b. http://earthquake.usgs.gov/eqcenter/ (the FCCOC receives email alerts)
   c. https://hsin.dhs.gov
2. Federal, State, Local Agency Reports
3. Review NORS
4. Gather data for possible ESRI geo-locating of communications assets:
   a. PSAPs
   b. State Emergency Operations Centers
   c. Broadcasters (AM, FM, TV, foreign, and designate EAS)
   d. Comms/internet switches
   e. Cell towers

SITREP Email Text

1. Use previous event SITREP as template (sample- Appendix A)
2. Copy/paste map if available (use NWS map for weather and all other events use DHS SITREP map)
3. Under the appropriate sections, list information similar to what exists in the template
4. If Disaster Information Reporting Systems (DIRS) is activated, copy/paste report to end of SITREP.

The SITREP is color-coded using the following guidelines:

a. New items – regular blue Arial in 11p
b. Previously reported *but* still active items – regular black Arial in 11p
c. Delete obsolete non-active items

Create TEAMS chat room

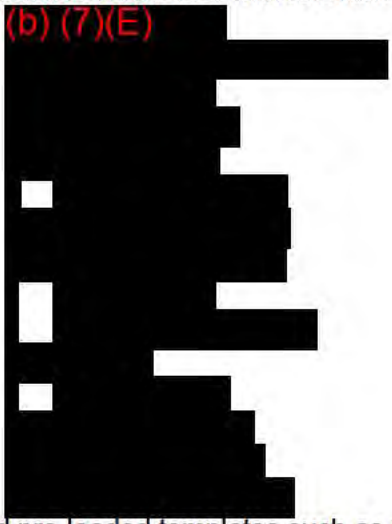
1. Invite OEM Incident management Team
2. Others should be added as the event unfolds

Create Outlook and "K" Drive Event Folders (for FCCOC use only)

1. Place all emails pertaining to the event in the specified Outlook folder
2. Place all information relevant to the event in the (b) (7)(E) folder

Create SharePoint Folder

1. If event warrants, create a SharePoint folder on the IMT site
2. (b) (7)(E)
3. Populate event folder with relevant sub-folders as needed



4. Add pre-loaded templates such as SITREPS, Spectrum scans, PSAP status Public Notices and Battle Rhythm to sub-folders
5. Preload SharePoint Planner with B/O IMT checklist taskings

Establish Event Battle Rhythm

1. Use previous event Battle Rhythm as a guide for current event
2. Editable version located in (b) (7)(E) as SOP34 Battle Rhythm
3. Update flow as required
4. Print and post on watch console

Requests for Information/Requests for Assistance (RFA/RFI)

1. Acknowledge receipt of request
2. Review request to determine level of response
3. Determine appropriate B/O IMT POC or agency the request should be handled by
4. Forward request to appropriate recipient

5. Create SharePoint Planner task to appropriate B/O
    a. RFA/RFI's to outside agencies will have planner task added to FCCOC.
6. Add information to daily Brief and event SITREP

Distribution

After ensuring information is accurate, current, and in the proper format:

1. During IMT activations, ensure FCC email distro group "IMT" is up to date; if updates are required, send list to email distro "Service-Center"
2. Copy/paste SITREP to email body and attach the SharePoint document
3. 1 hour prior to distribution, email to OEMD Chiefs for approval/comments. **Note-** this only applies to SITREPS released between 0700-1800. SITREPS released between 1800-0700 will be released without review/comment
4. Once approved for release, email to the following (expect additions/deletions depending on event):

PSHSB Bureau Chiefs
PSHSB Division Chiefs
PSHSB Chief of Staff
PSHSB/DHS Liaison
PSHSB/NORS Team
PSHSB/ABC
PSHSB Public Affairs Officer
FCCOC and HFDF Directors
Affected EB offices
Designated FCC field personnel (roll call, outreach, etc.)
When directed:
(b) (7)(E)
Incident Management Team

Updates

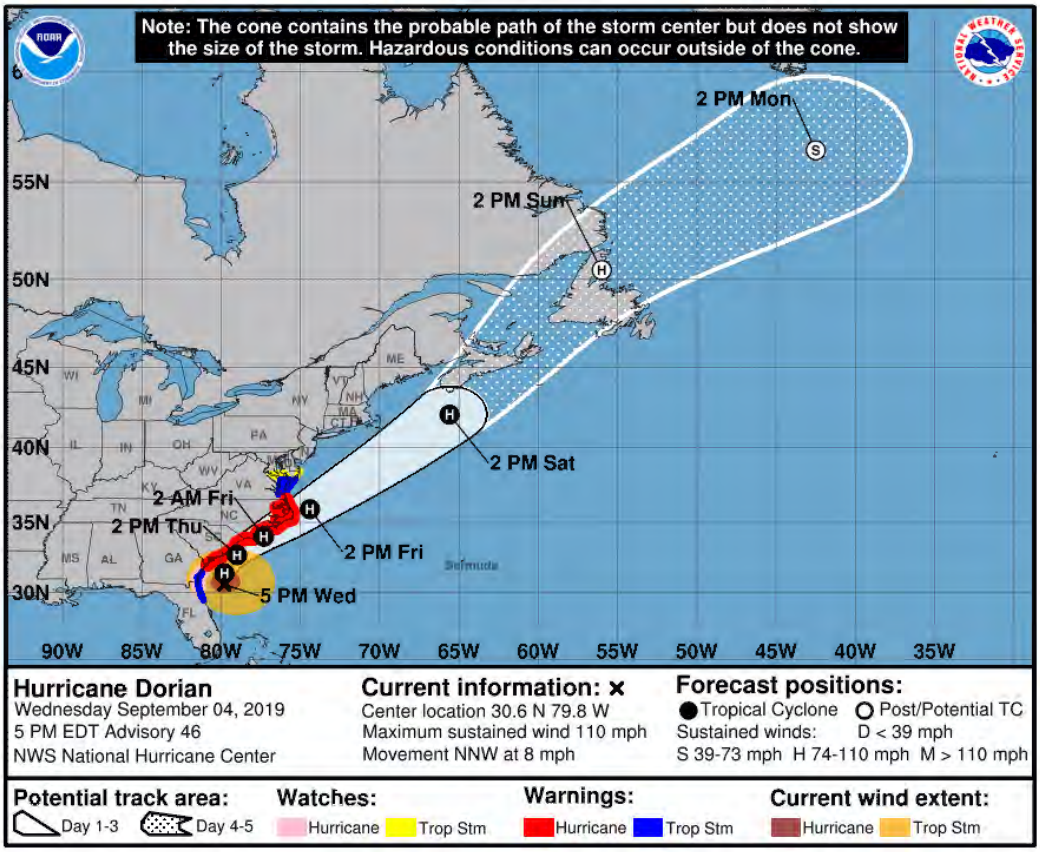
After initial reporting, updates will be sent only if there are significant changes to the report ***or*** daily SITREP requirements are established, in which case it will mirror the first SITREP. Noteworthy changes include:

- Reported telecommunications outages
- PSAP status
- STA/RFA/RFI requests and status

(Appendix A- SITREP)

FCC Hurricane Dorian Report 9/22/21 (initial)

Future updates in blue; underlined blue are hyperlinks to expanded information



Hurricane Dorian located 150 miles S of Charleston, NC moving NNW at 8 mph with winds of 110 mph

- Storm forecast
- Warnings & watches:

FCC Summary:

- IMT activated: _____; Deactivated _____
  - Daily meetings:
    - 0800- OEMD operations sync in Teams
    - 1230- FEMA Senior Leaders VTC/call 1230
    - 1400- NCC Government/Industry call
    - 1500- FEMA Reg VI call
    - 1500- FCC IMT in Teams
- FCC Hurricane Web Page
  - Public Notices issued: (0) new; (0) total
  - Orders/waivers granted: (0) new; (0) total
- Emergency STA Tracker
  - (0) new; (0) total
- Request for Assistance (RFA)/Request for Information (RFI)
  - (0) new; (0) total
- IMT SharePoint

- WTB Coverage Map and HiFLD Data
- Deployed personnel: (0)
    - 2 under FEMA….

DIRS: Activated 9/15 for 3 counties in LA

- Wireline:
    - 3 switching…
    - 3 on backup power
- Wireless:
    - 3 cell sites out of service
    - 3 on backup power
- PSAPS:
    - None out of service
- Broadcasters
    - None out of service

Over-the-Air monitoring

- **HFDFC:**
    - AM radio scans of GA/SC/NC coastal areas
        - 6 of 11 stations observed broadcasting as of 9/5 0849 EDT
- **Roll Call/NSREN**
    - Baseline surveys completed in LA, MS, and AL
    - Team conducting surveys on New Orleans

Bureau/Office Coordination

- **CGB**
- **EB**
- **IB**
- **MB**
- **OET**
- **WCB**
- **WTB**

Industry Updates:

- **AT&T web page**
- **T-Mobile web page**
- **Verizon web page**
- **Comcast web page**

Coordination/Outreach:

FEMA Reg VI:

NSC:

IMT and FCCOC Daily Battle Rhythm			
TIME	**ACTION**	**DETAILS**	**OPS SIGN**
24/7	**Ops Responsibilities**	• Monitor Teams event and Ops chat rooms • Ensure daily Brief and SITREP are always open for updates • Update planners and trackers as required • Update and print Daily Battle Rhythm for sign offs as required • Ensure email traffic is properly categorized prior to moving to appropriate folders • Send FEMA, CISA, and NCC SITREPS to Daily Brief and IMT as "FYSA" in subject line	
0800	OEMD Ops Sync Teams Call	• IMT Lead will host Team's chat room • Ops does not attend	
0845	HFDF AM Survey Results	• Save files to event SharePoint • Update Daily Brief and SITREP • Send to ESF2 using email templates	
0900	Daily Brief	• Review all Federal reports received for relevant information • Review event emails for relevant information • Update weather and DOJ Eagle-I power details • Send to Daily Brief, IMT, and EB Offices in affected areas	
1000	DIRS information due to CCR	• No action for Ops	
1100	Request B/O SITREP inputs	• Email B/O email template to IMT • Update SITREP with pertinent information	
1230	FEMA Senior Leaders Call	• FCC POC- (b) (6) • No action for Ops	
1400	NCC Gov/Industry Call	• FCC POC- (b) (6) • No action for Ops	
1400	"Government Only" DIRS report release	• Final report will be reviewed by (b) (6) and OCH • Save to SharePoint event folder • Use email template • Send to Daily Brief, IMT, EB Offices in path, NCC	
1500	IMT Teams Call	• IMT Lead will host Team's chat room • If available, Ops will brief latest weather and new RFA/RFI's	
1500	FEMA Region VI Call	• FCC POC- (b) (6) • No action for Ops	
1700	SITREP input due	• Finalize SITREP with all B/O inputs • Send to (b) (6) for review (include SharePoint link)	
1600	"Public" DIRS report release	• Final report will be reviewed by (b) (6) and OCH • Save to SharePoint event folder • Send to Daily Brief, IMT, EB Offices in path, NCC	
1800	SITREP Release	• Save to SharePoint event folder • Use email template • Send to Daily Brief, IMT, EB Offices in path, NCC	