

EFFECTIVE DATE NOTE: At 78 FR 40613, July 5, 2013, § 64.5110 was added. This section contains information collection and record-keeping requirements and will not become effective until approval has been given by the Office of Management and Budget.

**§ 64.5111 Notification of customer proprietary network information security breaches.**

(a) A TRS provider shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The TRS provider shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b) of this section. The TRS provider shall file a copy of the notification with the Disability Rights Office of the Consumer and Governmental Affairs Bureau at the same time as when the TRS provider notifies the customers.

(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the TRS provider shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at <http://www.fcc.gov/eb/cpni>.

(1) Notwithstanding any state law to the contrary, the TRS provider shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (b)(2) and (3) of this section.

(2) If the TRS provider believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (b)(1) of this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The TRS provider shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the TRS provider not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the TRS provider when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the TRS provider, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by TRS providers.

(c) *Customer notification.* After a TRS provider has completed the process of notifying law enforcement pursuant to paragraph (b) of this section, and consistent with the waiting requirements specified in paragraph (b) of this section, the TRS provider shall notify its customers of a breach of those customers' CPNI.

(d) *Recordkeeping.* All TRS providers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. TRS providers shall retain the record for a minimum of 2 years.

(e) *Definition.* As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

(f) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation,

order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

EFFECTIVE DATE NOTE: At 78 FR 40613, July 5, 2013, §64.5111 was added. This section contain information collection and record-keeping requirements and will not become effective until approval has been given by the Office of Management and Budget.

APPENDIX A TO PART 64—TELECOMMUNICATIONS SERVICE PRIORITY (TSP) SYSTEM FOR NATIONAL SECURITY EMERGENCY PREPAREDNESS (NSEP)

*1. Purpose and Authority*

a. This appendix establishes policies and procedures and assigns responsibilities for the National Security Emergency Preparedness (NSEP) Telecommunications Service Priority (TSP) System. The NSEP TSP System authorizes priority treatment to certain domestic telecommunications services (including portions of U.S. international telecommunications services provided by U.S. service vendors) for which provisioning or restoration priority (RP) levels are requested, assigned, and approved in accordance with this appendix.

b. This appendix is issued pursuant to sections 1, 4(i), 201 through 205 and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i), 201 through 205 and 303(r). These sections grant to the Federal Communications Commission (FCC) the authority over the assignment and approval of priorities for provisioning and restoration of common carrier-provided telecommunications services. Under section 706 of the Communications Act, this authority may be superseded, and expanded to include non-common carrier telecommunication services, by the war emergency powers of the President of the United States. This appendix provides the Commission's Order to telecommunication service vendors and users to comply with policies and procedures establishing the NSEP TSP System, until such policies and procedures are superseded by the President's war emergency powers. This appendix is intended to be read in conjunction with regulations and procedures that the Executive Office of the President issues (1) to implement responsibilities assigned in section 6(b) of this appendix, or (2) for use in the event this appendix is superseded by the President's war emergency powers.

c. Together, this appendix and the regulations and procedures issued by the Executive Office of the President establish one uniform system of priorities for provisioning and restoration of NSEP telecommunication services both before and after invocation of the President's war emergency powers. In order

that government and industry resources may be used effectively under all conditions, a single set of rules, regulations, and procedures is necessary, and they must be applied on a day-to-day basis to all NSEP services so that the priorities they establish can be implemented at once when the need arises.

\*In sections 2(a)(2) and 2(b)(2) of Executive Order No. 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions" April 3, 1984 (49 FR 13471 (1984)), the President assigned to the Director, Office of Science and Technology Policy, certain NSEP telecommunication resource management responsibilities. The term "Executive Office of the President" as used in this appendix refers to the official or organization designated by the President to act on his behalf.

*2. Applicability and Revocation*

a. This appendix applies to NSEP telecommunications services:

(1) For which initial or revised priority level assignments are requested pursuant to section 8 of this appendix.

(2) Which were assigned restoration priorities under the provision of FCC Order 80–581; 81 FCC 2d 441 (1980); 47 CFR part 64, appendix A, "Priority System for the Restoration of Common Carrier Provided Intercity Private Line Services"; and are being resubmitted for priority level assignments pursuant to section 10 of this appendix. (Such services will retain assigned restoration priorities until a resubmission for a TSP assignment is completed or until the existing RP rules are terminated.)

b. FCC Order 80–581 will continue to apply to all other intercity, private line circuits assigned restoration priorities thereunder until the fully operating capability date of this appendix, 30 months after the initial operating capability date referred to in subsection d of this section.

c. In addition, FCC Order, "Precedence System for Public Correspondence Services Provided by the Communications Common Carriers" (34 FR 17292 (1969)); (47 CFR part 64, appendix B), is revoked as of the effective date of this appendix.

d. The initial operating capability (IOC) date for NSEP TSP will be nine months after release in the FEDERAL REGISTER of the FCC's order following review of procedures submitted by the Executive Office of the President. On this IOC date requests for priority assignments generally will be accepted only by the Executive Office of the President.

*3. Definitions*

As used in this part: