The Commission further notes that cyber threats to network end users also threaten the abilities of the service provider's network to function as designed and to be available when required. Such threats include, for example, the proliferation of botnets and from "MAC spoofing," a technique whereby cyber hackers remotely change an assigned Media Access Control address of a network device to a different one, allowing the bypassing of access control lists on servers or routers, either "hiding" a computer on a network or allowing it to impersonate another computer. Therefore, the Commission seeks comment on steps that service providers should take, if any, to help detect and respond to threats to end users that take place *on or through* the service provider's network, and the extent to which best practices in this area would enhance detection and maximize effectiveness of response.

Procedural Matters

Ex Parte Presentations. This matter will be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. *See* 47 CFR 1.1200 & 1.1206. Although a Notice of Inquiry proceeding is generally exempt from the *ex parte* rules, the Commission finds that the public interest is best served by treating this critical cyber security matter as a "permit-but-disclose" proceeding. *See* 47 CFR 1.1200(a), 1.1204(b)(1). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentations must contain summaries of the substance of the presentations and not merely a listing of the subjects discussed. More than a one- or two-sentence description of the views and arguments presented is generally required. Other rules pertaining to oral and written *ex parte* presentations in permit-but-disclose proceedings are set forth in § 1.1206(b) of the Commission's rules, 47 CFR 1.1206(b).

Comment Filing Procedures. Comments may be filed using: (1) The Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies. *See Electronic Filing of Documents in Rulemaking Proceedings,* 63 FR 24121 (1998). Comments may be filed electronically using the Internet by accessing the ECFS: *http://fjallfoss.fcc.gov/ecfs2/* or the Federal eRulemaking Portal: *http://www.regulations.gov.* Parties who choose to file by paper must file an original and four copies of each filing.

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. Effective December 28, 2009, 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. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes 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.

Ordering Clause

Accordingly, it is ordered that, pursuant to sections 1, 4(i), 4(j), 4(o) and 7(b), 403 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i)–(j) & (o), 157(b) and 403, this Notice of Inquiry is adopted.

Federal Communications Commission.

Marlene H. Dortch,

Secretary.

[FR Doc. 2010–11162 Filed 5–10–10; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Chapter I

[PS Docket No. 10–92; FCC 10–62]

Effects on Broadband Communications Networks of Damage To or Failure of Network Equipment or Severe Overload

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: Consistent with the recommendations of the National Broadband Plan, the Federal Communications Commission (Commission or FCC) adopted this Notice of Inquiry to seek comment on the present state of survivability in broadband communications networks and to explore potential measures to reduce network vulnerability to failures in network equipment or severe overload conditions, such as would occur in natural disasters, pandemics, and other disasters or events that would restrain our ability to communicate. The Commission seeks comment broadly on the ability of existing networks to withstand localized or distributed physical damage, including whether there is adequate network redundancy and the extent of survivability of physical enclosures in which network elements are located, and severe overloads.

DATES: Comments are due on or before June 25, 2010 and reply comments are due on or before July 26, 2010.

ADDRESSES: Comments and reply comments may be filed using: (1) The Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies.

Comments and reply comments may be filed electronically using the Internet by accessing the ECFS: *http://fjallfoss.fcc.gov/ecfs2/* or the Federal eRulemaking Portal: *http://www.regulations.gov.*

Parties who choose to file by paper can submit filings 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. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes 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. Parties who choose to file by paper must file an original and four copies of each filing.

Parties wishing to file materials with a claim of confidentiality should follow the procedures set forth in § 0.459 of the Commission's rules. Confidential submissions may not be filed via ECFS but rather should be filed with the Secretary's Office following the procedures set forth in 47 CFR 0.459. Redacted versions of confidential submissions may be filed via ECFS.

FOR FURTHER INFORMATION CONTACT: John Healy, Communications Systems Analysis Division, Public Safety and Homeland Security Bureau at 202–418–2448 or Jeffery Goldthorp, Chief, Communications Systems Analysis

Division, Public Safety and Homeland Security Bureau at 202–418–1096.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Notice of Inquiry NOI in PS Docket No. 10–92, FCC 10–62, adopted and released on April 21, 2010. The complete text of this document is available for inspection and copying during normal business hours in the FCC Reference Information Center, Portals II, 445 12th Street, SW., Room CY–A257, Washington, DC 20554. This document may also be purchased from the Commission's duplicating contractor Best Copy and Printing, Inc., Portals II, 445 12th Street, SW., Room CY–B402, Washington, DC 20554, telephone (800) 378–3160 or (202) 488–5300, facsimile (202) 488–5563, or via e-mail at *fcc@bcpiweb.com.* It is also available on the Commission's Web site at *http://www.fcc.gov.* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice), 202–418–0432 (tty).

Synopsis of the Notice of Inquiry

The American Recovery and Reinvestment Act of 2009 (hereinafter "ARRA") directed the Commission to prepare a National Broadband Plan ("NBP" or "Plan") and report that plan to Congress. In particular, ARRA required the Commission to explore ways in which broadband infrastructure and services can "advance consumer welfare * * * public safety and homeland security * * * and other national purposes."

In response to a number of public notices issued as part of the NBP proceeding, the Commission received a wealth of commentary on the rapidly increasing importance of wireline and wireless broadband communications networks to consumers, businesses, emergency responders, and government agencies. A number of these comments focused on the importance of broadband survivability. Based on these comments and independent research conducted by Commission staff, the NBP laid out numerous proposals to ensure that our nation's critical broadband infrastructure can serve the current and future needs of our citizens in a consistent and reliable fashion.

Consistent with the recommendations of the NBP, the Commission adopted this Notice of Inquiry to enhance its understanding of the present state of survivability in broadband communications networks and to explore potential measures to reduce network vulnerability to failures in network equipment or severe overload conditions, such as would occur in natural disasters, pandemics, and other disasters or events that would restrain our ability to communicate. The Commission seeks comment broadly on the ability of existing networks to withstand localized or distributed physical damage, including whether there is adequate network redundancy and the extent of survivability of physical enclosures in which network elements are located, and severe overloads.

Reliance on broadband communications networks is increasing across all elements of our society and all sectors of our economy. For example, IP-based telephony services have penetrated into the consumer and enterprise markets at a breakneck pace, in many cases without the end-users even knowing that a major technology change has occurred. People are no longer tied to a single public-switched telephone network (PSTN), but communicate through a wide range of interconnected networks (*e.g.,* cable networks, fiber networks, local exchange carriers, licensed wireless broadband communications networks and unlicensed wireless internet service providers). As Americans increasingly rely on broadband communications networks for voice, video, data, and other communications services, the reliability and survivability of broadband communications networks becomes an even more critical factor in the safety, security, and well-being of the American people.

The FCC realizes that the increasing use of broadband communications networks for telecommunications-type services has blurred the distinction between the PSTN and IP-based broadband communications networks. Consequently, the Commission believes it important that it better understand the implications that this migration will have on the communications survivability of our voice and broadband communications networks.

Consumers, businesses, and government agencies increasingly rely on broadband communications networks to supply voice, video, and data service to fixed and mobile sites. For example, comments received in the National Broadband Plan proceeding indicate levels of broadband adoption ranging from 47% for rural residences to 79% for non-rural businesses. The network infrastructure required to support these diverse needs is extensive and complicated. In some instances long-term collaboration between telecommunications providers and other major enterprises has led to the development of robust networks with purpose-built survivability features. The Commission is concerned, however, that these features may not adequately ensure the survivability of all types of broadband service throughout the country, including in lesser developed or sparsely populated areas.

Broadband core networks are generally presumed to be quite survivable. Survivability is generally weaker in segments of communications networks closer to the network edge, however. In light of the ever-growing centrality of broadband communications it is imperative that we understand the resilience and survivability of our national broadband infrastructure. The Commission seeks comment, analysis, and information on the present state of broadband network survivability to three broad classes of harm: (1) Physical damage (whether due to malevolent acts, accidents, or *force majeure*), (2) inadequate redundancy, and (3) severe network overload. The Commission also seeks comment as specifically described below.

Enhancing our understanding of the state of survivability in broadband communications networks and exploring potential measures to reduce network vulnerabilities furthers the Commission's core purposes as set forth in section 1 of the Communications Act: (1) The establishment of "a rapid, efficient, Nation-wide and world-wide wire and radio communication service with adequate facilities," (2) "the national defense," and (3) "promoting safety of life and property through the use of wire and radio communication." The Commission seeks comment on the strongest sources of authority to act in this regard should it choose to do so, and asks commenters to address whether different sources of authority would be required with regard to different types of communications providers.

For example, the Commission seeks comment on whether it has authority under Title II and Title III to adopt specific measures to reduce network vulnerabilities should it choose to do so. In addition, the Commission seeks comment on whether the Commission could, if necessary, exercise ancillary authority to reduce network vulnerabilities, should the Commission choose to do so. In particular, the Commission seeks comment on the scope of its ancillary authority with regard to the matters described in this NOI in light of the recent decision of the United States Court of Appeals for the District of Columbia Circuit in *Comcast Corporation* v. *FCC.*

The Commission seeks comment on the survivability features and risks presented by the physical architecture of current broadband communications networks. What are the major single points of failure in broadband architectures (for example, edge router, gateway router, transport links, cell sites, and VoIP servers)? What are the impacts of failure these points? What measures do communications providers take to minimize the presence of single points of failure in broadband architectures? Under what conditions might these measures not be followed? What operational awareness do broadband service providers have on these dependencies? For example is the state of transport link diversity generally known and tracked by a broadband service provider? Do service providers account vulnerability of assets to specific threats? Is the incidence of single points of failure greater or lesser for small service providers and/or network operators? What special provisions are made to ensure the survivability of network services to critical response agencies like public safety answering points (PSAPs)? What provisions are made to ensure the survivability of cell sites relied on by first responders? Should traffic to critical response agencies or for critical services be prioritized? What other aspects of physical architecture create vulnerabilities in broadband communications networks? Besides single points of failure, are there dual failures that could impact a large number of users for an extended period of time? What should be the FCC's role in reducing single points of failure in broadband communications networks? What should the FCC's role be in increasing the level of redundancy in broadband communications networks taking into consideration the tradeoffs between potential regulatory burdens and the benefits of increased survivability?

In addition to network architecture, the Commission seeks comment on the survivability of physical facilities in which network elements are located. At the outset, the Commission notes that the Network Reliability and Interoperability Council (NRIC) adopted a set of best practices for communications physical security. What are the most effective and widely deployed NRIC physical security best practices? What policies are typically put in place to ensure adherence to relevant NRIC physical security best practices? How are decisions made about when not to apply NRIC best practices? Is the present level of protection adequate, and, if so, by what measure? If not, what else should be done and how should this be accomplished? In addition, what other structural, mechanical, environmental or electrical standards are utilized in the construction of facilities that house broadband network elements? What should the FCC's role be in encouraging the implementation of security best practices?

The Commission also seeks comment on the risks posed by network facility co-location. For example, does the co-location of network hardware in "carrier hotels" or "SuperNodes" represent a significant vulnerability of networks to physical attack or natural disaster? How widespread is this practice? What steps have been taken to ensure redundancy and diversity of physical network links to and from these facilities? Are these redundancies adequate at the metro, national, and international scales? Are security standards at these facilities adequate and uniformly enforced? What should the FCC's role be in the utilization of security standards for co-located network hardware? Finally, are the network elements housed in such facilities commonly protected by redundant elements in physically separated locations and will adequate power be available in an emergency? If not, how widespread is the lack of redundancy? What should the FCC's role be in increasing the level of redundancy for co-located network elements?

Redundancy is used in communications networks to improve survivability. Redundancy failures occur when a network is unable to route traffic over an alternate link when the primary or most desirable link is down. In the public-switched telephone network (PSTN), for example, switches, routers, and multiplexers often protect against service interruption due to one or more physical link failures by intelligently re-routing traffic around the failed link although calls that are in progress may be lost. Traditional telecommunications networks use monitoring and alarms to verify redundancy. Occasionally the re-routing fails to occur because the monitoring equipment does not recognize the physical link failure or because the re-routing equipment fails to execute the re-route. In addition, the cause of the initial link failure may also affect the redundant link, resulting in its failure. The Commission is concerned that the level of redundancy and the effectiveness of that redundancy in routing around failures may be inadequate in broadband communications networks. The Commission is also concerned that the quality of service (QoS) for the rerouted traffic is adequate.

The Commission therefore seeks comment on the risk of physical link failures along with the resulting risk of redundancy failures in broadband communications networks. For example, to what extent are core and edge network links protected with "dark" backup links? Are there instances where backup circuit paths occupy the same physical link as a primary circuit path? If so, how prevalent is this practice and what information, systems, or procedures might help to eliminate it? How best can the FCC help to prevent or resolve such problems? To what extent is switching and routing capacity in broadband communications networks protected by redundant systems or reserve switching capacity? Does good business practice dictate some minimum level of reserve switching capacity for a given network? If so, how is that capacity derived? Are the protection mechanisms themselves in broadband communications networks reliable? Are there failure mechanisms that will affect both the primary path and the back-up path? Finally, how can the FCC enhance the chances that redundancy works in broadband communications networks without unduly burdening network operators?

Large-scale events such as pandemics or bioterror attacks may cause dramatic changes in broadband usage patterns as traffic that is ordinarily confined within enterprise or academic networks or passed between enterprise-grade access networks suddenly shifts onto residential-access networks. If residential access networks are unprepared or insufficiently resourced for such changes, the resulting network congestion could threaten the orderly functioning of our economy and prevent citizens from accessing critical public safety services such as 911 call centers. What can be learned from recent events that, while not catastrophic, resulted in a surge of telecommuting (*e.g.,* the recent heavy snowstorms in the Mid-Atlantic States)?

In order to better understand the risks associated with sudden shifts of network traffic during pandemics and similar events, the Commission seeks comment on the ability of broadband access networks (*i.e.,* cable, DSL, fiber-to-the-home, etc.) to maintain effective operation during severe network congestion or overload. For example, is the capacity of residential access networks sufficient to handle sudden surges in use? To what degree? To the extent that network capacity is insufficient or networks are

"oversubscribed," what methods and procedures are in place to handle these overloads and to rapidly apply network resources to where they are needed? What are the limits to these network management techniques? For example, is there a need for ways to prioritize broadband traffic during emergencies? Are some network segments or geographic areas more vulnerable than others? The Commission also seeks detailed data on past instances: When outbreaks of influenza have closed schools in a given area, what changes were observed in residential access network traffic, and how did these changes affect the networks? Should the FCC collect data on network usage during such events?

As our broadband infrastructure continues to grow and mature, the Commission is committed to ensuring that it stands ready to support the myriad uses dreamed up by American innovators and enterprises. This Notice of Inquiry is a critical first step toward understanding survivability of our broadband communications networks to all types of failures and severe traffic overloads. The Commission looks forward to collaborating with consumers, businesses, and network operators to improve and secure our broadband infrastructure for the future.

Accordingly, *it is ordered that,* pursuant to sections 1, 4(i), 4(j), 4(o) and 7(b) of the Communications Act of 1934, 47 U.S.C. 151, 154(i)–(j) & (o), and 157(b) (2006), this Notice of Inquiry is adopted.

Federal Communications Commission.

Marlene H. Dortch,

Secretary.

[FR Doc. 2010–11159 Filed 5–10–10; 8:45 am]

BILLING CODE 6712–01–P

DEPARTMENT OF TRANSPORTATION

Office of the Secretary

49 CFR Part 40

[Docket OST–2008–0088]

RIN OST 2105–AE01

Procedures for Transportation Workplace Drug and Alcohol Testing Programs

AGENCY: Office of the Secretary, DOT.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Transportation is proposing only to extend the date for the mandatory use of our recently updated Alcohol Testing Form (ATF) to January 1, 2011. The revised ATF went into effect on February 25, 2010 with a mandatory use date of August 1, 2010. After publishing the February 25 revisions, we learned that vendors and users of the ATF will not be able to deplete their current supply of ATFs by August 1, 2010. Therefore, in order to assist the transportation industries and their service agents in their efforts to be economically efficient and more environmentally "green," we are seeking public comment to extend the mandatory use date to January 1, 2011.

DATES: Comments to the notice of proposed rulemaking should be submitted by May 26, 2010. Late-filed comments will be considered to the extent practicable.

ADDRESSES: To ensure that you do not duplicate your docket submissions, please submit them by only one of the following means:

- *Federal eRulemaking Portal:* Go to *http://www.regulations.gov* and follow the online instructions for submitting comments.
- *Mail:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Ave., SE., West Building Ground Floor, Room W12–140, Washington, DC 20590–0001;
- *Hand Delivery:* West Building Ground Floor, Room W12–140, 1200 New Jersey Ave., SE., between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329.

Instructions: You must include the agency name and docket number DOT–OST—or the Regulatory Identification Number (RIN) for the rulemaking at the beginning of your comments. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

FOR FURTHER INFORMATION CONTACT: For program issues, Bohdan Baczara, Office of Drug and Alcohol Policy and Compliance, 1200 New Jersey Avenue, SE., Washington, DC 20590; (202) 366–3784 (voice), (202) 366–3897 (fax), or *bohdan.baczara@dot.gov* (e-mail).

SUPPLEMENTARY INFORMATION:

Background and Purpose

On February 25, 2010, the Department published a final rule [75 FR 8528] which updated the Alcohol Testing Form (ATF). The Department anticipated that employers and alcohol testing technicians may currently have a large supply of old ATFs and to avoid unnecessarily wasting these forms, the Department permitted the use of the old ATF until August 1, 2010. Employers were authorized to begin using the updated ATF immediately.

Since the final rule was published, the Department became aware that some vendors of the ATF might not be able to deplete their current supply of the ATFs before the August 1, 2010 implementation date. In light of this new information and so as not to have the industry waste forms, the Department is proposing to extend the implementation date to January 1, 2011. The Department seeks your comments only about this new implementation date.

Regulatory Analyses and Notices

The statutory authority for this proposed rule derives from the Omnibus Transportation Employee Testing Act of 1991 (49 U.S.C. 102, 301, 322, 5331, 20140, 31306, and 45101 *et seq.*) and the Department of Transportation Act (49 U.S.C. 322).

This proposed rule is a non-significant rule both for purposes of Executive Order 12886 and the Department of Transportation's Regulatory Policies and Procedures. The Department certifies that it will not have a significant economic effect on a substantial number of small entities, for purposes of the Regulatory Flexibility Act. The Department makes these statements on the basis that by extending the implementation date of the new form, this rule will not impose any significant costs on anyone. The costs of the underlying Part 40 final rule were analyzed in connection with its issuance in December 2000. Therefore, it has not been necessary for the Department to conduct a regulatory evaluation or Regulatory Flexibility Analysis for this proposed rule. The alcohol testing form complies with the Paperwork Reduction Act. It has no Federalism impacts that would warrant a Federalism assessment.

List of Subjects in 49 CFR Part 40

Administrative practice and procedures, Alcohol abuse, Alcohol testing, Drug abuse, Drug testing, Laboratories, Reporting and recordkeeping requirements, Safety, Transportation.

Issued April 28, 2010, at Washington DC.

Jim L. Swart,

Director.

For reasons discussed in the preamble, the Department of Transportation proposes to amend 49 CFR part 40, Code of Federal Regulations, as follows: