Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of

Secure Internet Routing PS Docket No. 22-90

COMMENTS OF APCO INTERNATIONAL

The Association of Public-Safety Communications Officials, International (APCO),\(^1\) submits these comments in response to the Public Safety and Homeland Security Bureau’s Notice of Inquiry regarding secure internet routing.\(^2\) The Bureau seeks comment on vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP) and its impact on 9-1-1 calls, among other things.\(^3\)

The Commission asks whether stakeholders have attempted to measure or quantify the extent to which BGP hijacking poses a threat to life and property by disrupting 9-1-1 calls carried by providers of interconnected VoIP service.\(^4\) APCO welcomes this inquiry and appreciates the Commission’s attention to the potential impacts on 9-1-1. While some risks to public safety are evident, we look forward to reviewing the record to better understand the steps service providers have taken to prevent BGP hijacking that would redirect or otherwise disrupt 9-1-1 calls. In addition to the value these insights will provide for improving network security,

\(^1\)Founded in 1935, APCO is the nation’s oldest and largest organization of public safety communications professionals. APCO is a non-profit association with over 36,000 members, primarily consisting of state and local government employees who manage and operate public safety communications systems – including 9-1-1 Emergency Communications Centers (ECCs), emergency operations centers, radio networks, and information technology – for law enforcement, fire, emergency medical, and other public safety agencies.


\(^3\)Id.

\(^4\)Id. at para. 18.
information about these types of disruptions may help guide next steps for the revision of the Commission’s 9-1-1 outage reporting requirements.\(^5\)

In light of BGP vulnerabilities and other threats to reliability for public safety communications, networks supporting emergency communications should be designed for high reliability and redundancy. Among other things, this should mean network diversity with no single point of failure and cybersecurity measures incorporated as part of system design. As the Bureau examines BGP vulnerabilities, APCO encourages a comprehensive approach that addresses the many cyber challenges facing ECCs. For example, APCO supports further consideration of options to support cybersecurity for ECCs, such as the EC3 model described in the TFOPA report.\(^6\)

Finally, vulnerabilities threatening the security and integrity of BGP present risks to public safety that are not limited to 9-1-1 calls, such as emergency alerts and first responder communications. Given the unique public safety concerns present in the event of a cyber-attack on a 9-1-1 center or public safety communications systems, the Commission should ensure service providers implement appropriate security measures to protect emergency communications.

Respectfully submitted,

APCO INTERNATIONAL

By:

Jeffrey S. Cohen
Chief Counsel
(571) 312-4400 ext. 7005

---

\(^5\) See Comments of APCO International, PS Docket Nos. 15-80, 13-75, ET Docket No. 04-35 (filed July 30, 2021) (explaining that improved knowledge of the type and scope of network outages impacting 9-1-1 will help determine how to revise the rules on outage reporting thresholds and notification requirements).

April 11, 2022