Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
IMPLEMENTATION OF CSRIC III	)	DA 14-1066
CYBERSECURITY BEST PRACTICES	)	

To: Public Safety & Homeland Security Bureau

COMMENTS OF APCO

The Association of Public-Safety Communications Officials-International, Inc. ("APCO") hereby submits the following comments in response to the above-captioned *Public Notice*, released July 25, 2014, in which the Public Safety & Homeland Security Bureau seeks comments regarding the implementation and effectiveness of voluntary recommendations adopted by the third Communications Security, Reliability and Interoperability Council (CSRIC III) for Internet service providers (ISPs) to combat certain cybersecurity threats.

Founded in 1935, APCO is the nation's oldest and largest public safety communications organization. Most APCO members are state or local government employees who manage and operate communications systems -- including Public Safety Answering Points (PSAPs), dispatch centers, radio networks, and information technology -- for law enforcement, fire, emergency medical, forestry conservation, highway maintenance, disaster relief, and other public safety agencies.

APCO's comments are primarily in response to Question 5 in the *Public Notice,* and address the cybersecurity threat to PSAP operations, which directly impacts the safety of life and property. Question 5 asks:

> How effective are the recommendations at mitigating cyber risk when they have been implemented? Given the experiences gained in the past two years, are there alternatives to full implementation that could be more effective than full

implementation at mitigating cyber risk risks posed by botnets, DNS vulnerabilities, routing infrastructure vulnerabilities, and source address spoofing? On what basis do stakeholders believe that these alternatives are more effective than the CSRIC III recommendations? Do stakeholders undertake qualitative or quantitative evaluations of the effectiveness of these various approaches, or both?

CSRIC III's recommendations are solid and provide an excellent baseline. That said, only 24 months after their adoption, we are already seeing new threats and new vectors to old threats. Public safety entities have experienced hundreds of Telephony Denial of Service (TDoS) attacks in the past year, with national attention now being focused on mitigation and prevention. The difficulty has been that there are numerous actors, and many are located overseas where enforcement is difficult, if not impossible. In addition, new vectors to the TDoS attacks have been identified in only the last few months, indicating the ability of the perpetrators to be both adaptive and progressive when their initial vectors are uncovered and mitigation steps are taken. There must be response in kind with both prevention efforts (where possible) and mitigation strategies as events occur.

In addition to TDoS attacks, PSAPs in an IP environment have already seen attempts at Distributed Denial of Service (DDoS) attacks. As the number of PSAPs evolving to Next Generation 9-1-1 (NG9-1-1) increases, both the number of targets, and the potential impact, increases as well. PSAPs are not traditionally well schooled in cybersecurity and may need to give particular attention to both crafting and implementing new cybersecurity-related policies and practices. The ability of outside actors to re-route PSAP traffic could be catastrophic and result in missed calls, no response, and loss of life. This should not be overlooked.

Additional consideration should also be given to the growing use of "apps" as a means to communicate with PSAPs and public safety in general. Security concerns obviously increase whenever any type of Internet (or outside network) connection into a PSAP is required. Text-to-

9-1-1 via browser interface has been relatively well controlled by the primary vendors through use of secure VPN's. Unfortunately, app developers do not currently employ such methods or connectivity on a consistent basis.

Cybersecurity is a major concern of an APCO working group developing standards for the app interface. On February 25, 2014, APCO, in cooperation with FirstNet and the Department of Commerce, held a half-day workshop titled "Public Safety Mobile Application Security Requirements" attended by public safety practitioners, mobile application developers, industry experts, and government officials. In this first-of-its-kind workshop, attendees contributed their experience and knowledge to provide input in identifying security requirements for public safety mobile applications. A resulting Interagency Report developed by the National Institute of Standards and Technology, NISTIR 8018, describes the workshop and captures the input that was received from the workshop attendees. The public comment period ended on September 13, 2014, and a draft can be viewed at http://csrc.nist.gov/publications/drafts/nistir-8018/nistir_8018_draft.pdf. Furthermore, this document followed publication by APCO of its "Key Attributes of Effective Apps for Public Safety and Emergency Response," found at http://appcomm.org/wp-content/themes/directorypress/thumbs//AppComm_Key_Attributes.pdf, which includes references to security considerations.

In addition to these concerns, the creating of Emergency Services IP Networks (ESINets) and the linking of PSAPs and the public through these networks will also introduce some unique challenges. There have been a number of notable "SWATTING" incidents in the past year that have resulted in major responses by tactical teams, only to determine (after breaking down doors and placing all the occupants in temporary custody) that there was no emergency and that the SWATTING incident was perpetrated by actors either outside of the relevant state, or in some

cases outside of the U.S. Were even one of these incidents to have gone badly, lives could have been lost. These incidents have been effected by using available IP relay centers, which lack the ability to definitively locate and verify the identity of callers. When implemented, ESINets, whether IMS based or using other protocols, must include verifiable locations, identities and safeguards to fend off future SWATTING incidents. Interstate enforcement, and cooperation, are also key.

The ability to secure public safety sites, equipment, systems, and networks has never been more important. CSRIC III's work provides an opportunity to build on solid principles and enhance our ability to protect public safety communications in an ever changing, and increasingly threat-laden environment. In order to do so, we must be as creative as the perpetrators we are attempting to thwart.

Respectfully submitted,

APCO INTERNATIONAL

By: /s/
Robert M. Gurss
Senior Regulatory Counsel
(202) 236-1743 (m)
gurssr@apcomail.org

APCO Government Affairs Office
1426 Prince Street
Alexandria, VA 22314

September 26, 2014