Influencing Tech Policy

Internet2 CommEx 2024

Andrew Gallo, George Washington University

Mark Johnson, SpekiGroup, LLC

Anita Nikolich, University of Illinois-Urbana Champaign

Agenda

- Defining Tech Policy

- Areas of Interest to the R&E Community

- Purpose of Tech Policy Engagement

- Tech Policy Reading Group Recap

- Example of Successful Engagements

- Call to Action

What is Technology Policy?

Governance vs Standardization vs Policy/Regulation/Law

Governance: mostly internal and alignment focused

Standards: formal processes, guidelines, or specifications

Policy: regulation over current and emerging tech

Deeper Dive: Standardization

Developed by subject matter experts

Generally consensus-driven, cooperatively developed and adopted

R&E community tends to do a good job. Recent example:

- Participation in ASPA (Autonomous System Provider Authorization)
- Discussing R&E ‘quirks’ with RFC authors…this is good participation

But *who is communicating with regulators*? (Secure routing framework)

Standards Organizations Examples

Definitions: Policy & Regulation

- Formed by non-experts
- Imposed, top-down
- Global, National, Local
- Can be reactionary
- Can have unintended consequences
- Impacts individuals, society and public interest

Purpose of R&E Tech Policy Engagement

Understand issues prior to forced compliance

Translate technical knowledge into public good

Strengthen voice of Higher Ed on Capitol Hill

Represent unique niche of R&E community: data privacy, disinformation/truth, encryption, internet governance, etc

Who is Doing This & How?

-Quilt: Advocacy (i.e., FCC E-Rate)

-Institutions: Lobbying & Advocacy (~$75M annually); trend of hiring political professionals

-Researchers: Provide data and expertise. Disconnected from operations

-Individuals: RFI Responses, activism, data collection/analysis

Why Do We Need This?

There’s a Gap :

-Educause had been highly engaged

-Campuses have own engagements with Congresspeople and Federal agencies

-Researchers engage with policy but disconnected from Ops

Policy Areas for R&E Community

-Secure Infrastructure

White House 2023 National Cybersecurity Strategy

- Affordable Broadband

-Encryption

- App bans (ie TikTok)

-Content Moderation/Section 230

-Data Collection

GenAI, TikTok, EdTech and other apps

Avoid Sudden Impact for CIOs

TikTok bans on gov’t resources

ARIN Legacy Services Agreement example

Hidden compliance issues e.g. Chinese-made equipment restrictions on sourcing with gov’t funds

Data privacy compliance

Avoid Sudden Impact for CIOs

AT&T Copper/landline policy in California

- Impact on campus services: backups/OOB
- Emergency operations on campuses

What to do?

- How do I get this information?
- How do I know what policy will affect me?
- Who else on my campus or community cares?

Tech Policy Reading Group

Reading Group Recap

5 meetings:

- AI Regulation
  - **“The Surprising Thing A.I. Engineers Will Tell You if You Let Them”**
    - US vs. Europe

- Open Access Networks
  - **“How the NTIA Can Fund Future-Proof Open Access Fiber”**
  - **“Should Grant-funded Networks be Open-Access?”**
    - When federal dollars fund networks with requirements for “open access” networks.
    - Are R&E networks open?

Reading Group Recap

- TikTok Ban - Project Texas
  - “Project Texas: The Details of TikTok’s Plan to Remain Operational in the US”
    - Politics and mechanisms of a government ban of an application

- Network Neutrality, 2023
  - “FCC to Start Proceeding on Reestablishing Open Internet Protections”
    - What has changed since 2018?
    - Possible legal challenges if the rule is adopted

Reading Group Recap

- First Amendment and Social Media
  - “Silicon Valleys’ Speech: Technology Giants and the Deregulatory First Amendment”
    - Do social media companies have First Amendment rights?
    - Is the act of content moderation a protected free speech act?
    - How do social media companies compare to other media channels with respect to case law?
  - Highlight: Guest participant: Nick Nugent, UTenn Law Professor and ARIN NRO Number Council

Advocacy

Anyone can be an advocate.

Anyone can respond to RFIs.

Tech community should respond and give input!

NIST AI Risk Management Framework Request for Information (RFI) Example

Artificial Intelligence Risk Management Framework

A Notice by the National Institute of Standards and Technology on 08/24/2021

PUBLISHED DOCUMENT

AGENCY:

National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION:

Request for Information.

SUMMARY:

The National Institute of Standards and Technology (NIST) is extending the period for submitting comments relating to the NIST Artificial Intelligence Risk Management Framework (AI RMF or Framework) through September 15, 2021. In a Request for Information (RFI) that published in the **Federal Regster** on July 29, 2021 (86 FR 40810), NIST requested information to help inform, refine, and guide the development of the AI RMF. The Framework will be developed

DOCUMENT DETAILS

Printed version:
PDF

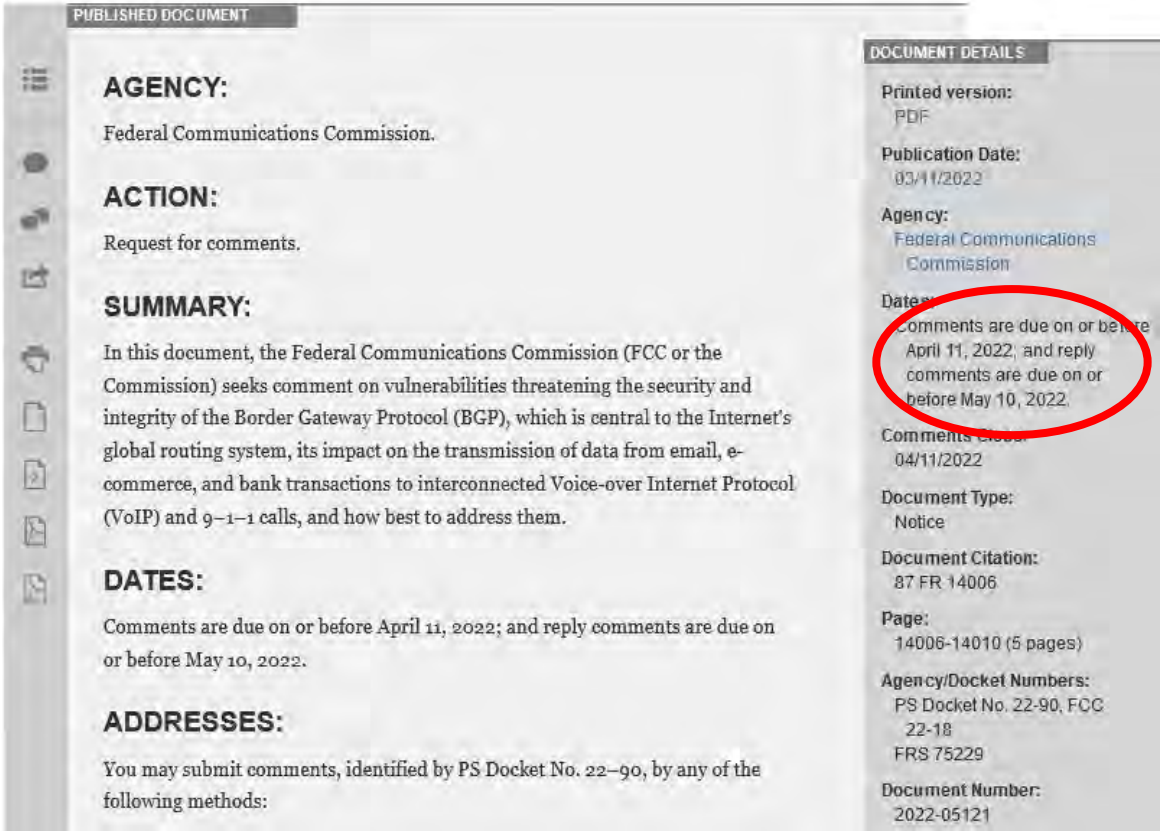
Publication Date:
08/24/2021

Agencies:
Department of Commerce
National Institute of Standards and Technology

Dates:
Comments in response to this notice must be received by 5:00 p.m. Eastern time on September 15, 2021. Written comments in response to the RFI should be submitted according to the instructions in the ADDRESSES and

Secure Routing Example

Federal Register:



PUBLISHED DOCUMENT

AGENCY:

Federal Communications Commission.

ACTION:

Request for comments.

SUMMARY:

In this document, the Federal Communications Commission (FCC or the Commission) seeks comment on vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the Internet's global routing system, its impact on the transmission of data from email, e-commerce, and bank transactions to interconnected Voice-over Internet Protocol (VoIP) and 9–1–1 calls, and how best to address them.

DATES:

Comments are due on or before April 11, 2022; and reply comments are due on or before May 10, 2022.

ADDRESSES:

You may submit comments, identified by PS Docket No. 22–90, by any of the following methods:

DOCUMENT DETAILS

Printed version:
PDF

Publication Date:
03/11/2022

Agency:
Federal Communications Commission

Dates:
Comments are due on or before April 11, 2022; and reply comments are due on or before May 10, 2022.

Comments Close:
04/11/2022

Document Type:
Notice

Document Citation:
87 FR 14006

Page:
14006-14010 (5 pages)

Agency/Docket Numbers:
PS Docket No. 22-90, FCC 22-18
FRS 75229

Document Number:
2022-05121

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Secure Internet Routing	)	PS Docket No. 22-90
	)	

NOTICE OF INQUIRY

Adopted: February 28, 2022 **Released: February 28, 2022**

Comment Date: 30 days after Federal Register Publication
Reply Comment Date: 60 days after Federal Register Publication

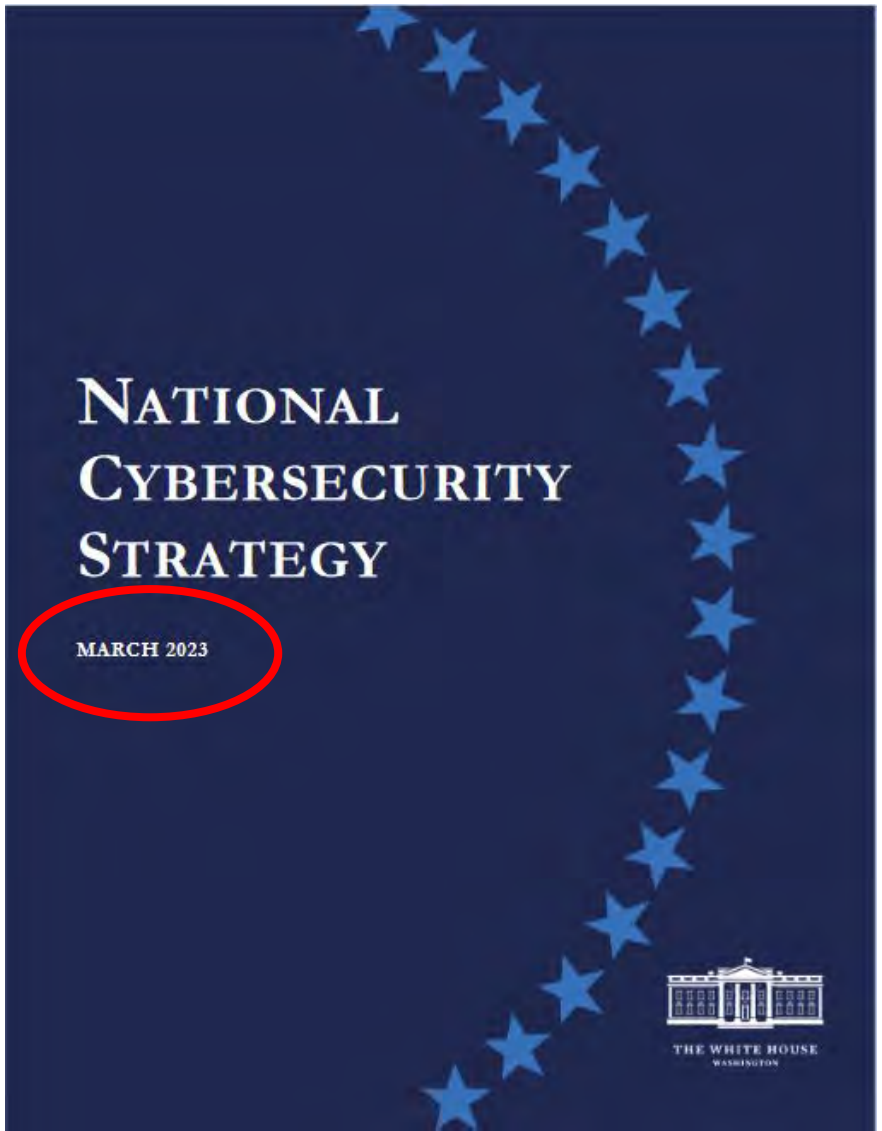
By the Commission:

I. INTRODUCTION

1. The Commission plays an important role in protecting the security of America's communications networks and critical infrastructure. The Commission, in tandem with its federal partners, has urged the communications sector to defend against cyber threats, while also taking measures to reinforce our Nation's readiness and to strengthen the cybersecurity of vital communications services and infrastructure, especially in light of Russia's escalating actions inside of Ukraine. Today, we build on those efforts. With this *Notice of Inquiry* (*Notice*), we seek comment on vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the Internet's global routing system, its impact on the transmission of data from email, e-commerce, and bank transactions to interconnected Voice-over Internet Protocol (VoIP) and 9-1-1 calls, and how best to address them.

2. BGP is the routing protocol used to exchange reachability information amongst independently managed networks on the Internet.[1] BGP's initial design, which remains widely deployed today, does not include security features to ensure trust in the information that it is used to exchange.[2] As

Reading the Tea Leaves Helps



STRATEGIC OBJECTIVE 4.1: SECURE THE TECHNICAL FOUNDATION OF THE INTERNET

Secure Routing Responses

FCC Notice of Inquiry (NOI): *In the Matter of Secure Internet Routing*

- 46 comments filed
- An analysis the routing security posture of top 25 Federal websites

FCC Network Neutrality 2023

- 52,000 comments filed
- Internet2 and Quilt respond advocating on behalf of R&E

Secure Routing: Responses and Actions

FCC July 2023 Workshop on Internet Routing System Security

-Internet2 Steve Wallace presented

PUBLIC NOTICE

Federal Communications Commission
45 L St., N.E.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: https://www.fcc.gov
TTY: 1-888-835-5322

DA 23-522

Released: June 16, 2023

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU TO HOST PUBLIC WORKSHOP ON BORDER GATEWAY PROTOCOL SECURITY ON JULY 31, 2023

PS Docket No. 22-90

The security of the Border Gateway Protocol (BGP) is central to the Internet's global routing system. By this Public Notice, the Public Safety and Homeland Security Bureau (PSHSB) announces that it will host a public workshop on BGP Security on Monday, July 31, 2023, starting at 9:30 am EDT. The event will build upon the robust record generated by the Commission's Notice of Inquiry to identify and discuss existing and potential safeguards to address BGP security issues.

The workshop will highlight the critical importance of addressing risks associated with BGP in light of the risk of consumer harm posed by unsecured Internet routing and explore effective security practices to mitigate these vulnerabilities. The workshop will feature the perspectives from a variety of stakeholders on the actions that have been taken to improve BGP security and a discussion about the potential for future actions for enhancing BGP security. For instance, the workshop will examine the viability of emerging BGP security advancements to address path validation and other approaches to lessen the risks currently inherent in interdomain routing. The workshop will include an opportunity for attendees to engage directly with presenters.

Secure Routing: Responses and Actions

2023 White House Cybersecurity Framework calls out Internet infrastructure protection

- Section 4.1 - Secure the Technical Foundation of the Internet
  - 4.1.4 “Accelerate the development, and standardization, and support the adoption of foundational Internet infrastructure capabilities and technologies.

White House Office of National Cyber Director (ONCD) guidance forthcoming

Call to Action: Purpose

- R&E technical community experts informing Higher Ed IT leadership
- Use our technical expertise to inform policy makers (legislators, regulators) *during* policy formation

Call to Action

- Continue to expand the monthly Tech Policy Reading Group
- Encourage RFI responses from R&E community
- Increase Engagement & Gain Traction
  - I2 SIG? BoF? mailing list?
- Collaboration with I2 External Relations Program Advisory Group (ERPAG) and other PAGs

Q&A/Thoughts/Feedback?

Is this a good idea?

Does this duplicate efforts?

How to best involve people?

Are there any specific policy efforts we should be following AND participating in?