AMPERE

Briefing:
White House National Cybersecurity Strategy

ONG-ISAC Biweekly Analyst Threat Call
March 8 2023

Introduction

- CEO, Ampere Industrial Security
- Former utility staff (telecommunications, water & electric)
- Drafter of NERC CIP standards and formal interpretations, current SCWG and SITES contributor
- First NERC CIP auditor in North America; Manager CIP Audits and Investigations (WECC)
- Contributor to NERC/ERO Auditor Manual and Guidance
- Speaker/contributor to multiple FERC Technical Committees, NOPRs and Orders
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, former Director, former Instructor and President Emeritus
- SANS Instructor: ICS456 - Essentials for NERC Critical Infrastructure Protection
- Contributor, DHS CISA Cross-Sector Cybersecurity Performance Goals (CPGs)
- NTIA/INL Software Bill of Materials (SBOM) Energy POC Stakeholders
- NARUC/NASEO Cybersecurity Advisory Team for State Solar (CATSS)
- DOE SETO/NREL Industry Advisory Board (IAB) for the Securing Solar for the Grid (S2G)
- DOE/NARUC Cybersecurity Advisory Group for for Distribution
- GCIP, CISSP-ISSAP, SSCP, CISA, CRISC, CEH, CVI

What Happened?

- White House issued National Cybersecurity Strategy (3/1/2023)
  - Companion Fact Sheet
- Well constructed; input from many parties
- Not a law, not an executive order, closer to a memorandum
- Five pillars
  - Defend Critical Infrastructure
  - Disrupt and Dismantle Threat Actors
  - Shape Market Forces to Drive Security and Resilience
  - Invest In a Resilient Future
  - Forge International Partnerships to Pursue Shared Goals
- Implementation (call to action)

“Fundamental Shifts”

- “We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.”

- “We must realign incentives to favor long-term investments by striking a careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future.”

Why now?

- Follows trend from current administration…
  - Executive Orders
  - 100-day sprints
  - National Security Memoranda
  - Cross-Sector Cyber Performance Goals
  - CIRCIA, CHIPS Act, Science Act, etc.
  - International ransomware coalition
- Last one was in 2018
- “While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes”

1. Defend Critical Infrastructure

- Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance;
- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services; and,
- Defending and modernizing Federal networks and updating Federal incident response policy

2. Disrupt and Dismantle Threat Actors

- Strategically employing all tools of national power to disrupt adversaries;
- Engaging the private sector in disruption activities through scalable mechanisms; and,
- Addressing the ransomware threat through a comprehensive Federal approach and in lockstep with our international partners.

3. Shape Market Forces to Drive Security and Resilience

- Promoting privacy and the security of personal data;
- Shifting liability for software products and services to promote secure development practices; and,
- Ensuring that Federal grant programs promote investments in new infrastructure that are secure and resilient.

4. Invest in a Resilient Future

- Reducing systemic technical vulnerabilities in the foundation of the Internet and across the digital ecosystem while making it more resilient against transnational digital repression;
- Prioritizing cybersecurity R&D for next-generation technologies such as postquantum encryption, digital identity solutions, and clean energy infrastructure; and,
- Developing a diverse and robust national cyber workforce

5. Forge International Partnerships to Pursue Shared Goals

- Leveraging international coalitions and partnerships among like-minded nations to counter threats to our digital ecosystem through joint preparedness, response, and cost imposition;
- Increasing the capacity of our partners to defend themselves against cyber threats, both in peacetime and in crisis; and,
- Working with our allies and partners to make secure, reliable, and trustworthy global supply chains for information and communications technology and operational technology products and services.

Summary Highlights

- Name and shame nation states as biggest threat
- Critical infrastructure sectors that don’t have regulation, probably will soon
- Shifting liability to software makers vs. consumers
- OT gets a legitimate mention
- Cyber-Informed Engineering (CIE, CCE)
- Cyber workforce
- Lighter on incident response, but CSRB

Challenges

- “…work with Congress…”
  - Vegas wouldn’t take these odds
- New regulation, legislation will be needed
  - Even reversal of some existing legal standing
- Lean on State regulatory functions
  - 50+ different opinions
- Administration may change in 2 years
  - What if we do a bunch of hard work and spend a lot of money and everything gets unwound in 2 years?

What should you do?

- Review the Cross-Sector Cyber Performance Goals (CPGs)
  - Assess your position against CPGs
  - Compare against any existing framework you are already using
- Assess all IT and OT interdependencies (re: Colonial example)
  - Could you do “intelligent islanding”
- Ramp up on the following:
  - Internal network security monitoring (INSM)
  - Incident response efforts (CSRB; CIRCIA)
  - Information sharing
- Expect more Executive Orders and other “levers”

Questions?

Email: pmiller@amperesec.com

Web: www.amperesec.com

LinkedIn: https://www.linkedin.com/in/millerpatrickc/

Twitter: @patrickcmiller

Mastodon: @patrickcmiller@infosec.exchange

Podcast: Critical Assets Podcast