White House Unveils Road Map For National Cybersecurity Strategy

JULY 14TH, 2023 BY DAVID ARIOSTO | 0 COMMENTS

CIPHER BRIEF REPORTING – In March, the Biden Administration unveiled its new cybersecurity strategy, instructing private entities to take more responsibility against would-be hackers targeting American infrastructure, business, and government agencies. On Thursday, the White House published the first version of a road map intended to detail just how it would roll out that strategy through 2026.

The 57-page document designated 16 sectors as U.S. critical infrastructure – including energy, health care, manufacturing, and financial services – in a step-by step plan that describes how the federal government plans to regulate digital security. The road map also identifies dozens of initiatives, with an emphasis on private sector coordination, and is structured — officials say — to evolve over time in a bid to better respond to both emerging threats and new policy initiatives.

"The implementation plan is a living document," Acting National Cyber Director Kemba Walden told reporters. "The National Cybersecurity strategy is meant to be enduring and is crafted to guide policy across the decisive decade in which we find ourselves …. [The] implementation Plan, on the other hand, will evolve whether in response to changing threat landscapes, or as initiatives are completed and we get follow on actions."

A key rationale, she said, is that "we know cyberattacks are going to happen."

"The downtime is going to be quick," Walden added, "so we need to figure out what investments we need to make."

Part of the rollout involves updating the National Cyber Incident Response Plan, meant to guide the national approach in dealing with cyber incidents with "clear guidance to external partners on the roles and capabilities of federal agencies in incident response and recovery."

Former Cyberspace Solarium Executive Director and Cyber Initiatives Group Principal Mark Montgomery told *The Record* that it is an "excellent effort to turn the rhetoric of the strategy into effective, measurable policy objectives," though expressed reservations for want of a "more full-throated approach to security in cloud computing with either regulation or collective standard setting objectives."

Looking for a way to get ahead of the week in cyber and tech? Sign up for the Cyber Initiatives Group Sunday newsletter to quickly get up to speed on the biggest cyber and tech headlines and be ready for the week ahead. Sign up today.

With cyber threats often emanating from state-sponsored entities in Russia, China, and North Korea, experts say the nature of such operations often take on decentralized characteristics in their attacks on American companies and interests that make prevention a more sophisticated endeavor, thus requiring a more coordinated U.S. approach.

This week's release also outlines the ways in which private companies are now expected to meet new standards established by federal agencies.

"While [the plan] does not intend to capture all cybersecurity activities being carried out by agencies, it describes more than 65 high-impact initiatives requiring executive visibility and interagency coordination that the Federal government will carry out to achieve the Strategy's objectives," the document said.

The nature of plan in part, stems from continued concerns over ransomware attacks akin to the breach of Colonial Pipeline, America's largest fuel conduit, which delivers nearly half the gasoline consumed on the East Coast, and which had to halt fuel deliveries for nearly a week after an attack in 2021. That strike was something former U.S. Director of the Cybersecurity and Infrastructure Security Agency (CISA) Chris Krebs, who is also a Cyber Initiatives Group Principal, described as a "wake-up call."

In the broader landscape prior to Thursday's release, CISA Executive Director Brandon Wales praised his agency's recent "wins," while also cautioning that "there's a lot more growth to do."

"A lot of that has to do with bringing more people into the fight."

Speaking during a recent Cyber Initiatives Group Summit, Wales said that "just a few months ago … [the agency] made over 100 notifications to organizations that have ransomware-related vulnerabilities on … internet accessible devices [tied to] a variety of critical infrastructure sectors," including "defense industrial base, energy, financial services, schools, hospitals, state and local governments."

Amidst recent changes, he noted that "companies will come to us" to notify of activity across a network, and that that collaboration is "really based upon that trust and partnership we have built." He added that "in this calendar year alone, we've done over 430 pre-ransomware notifications, both in the United States and including some overseas, working with our international partners."

The Cipher Brief hosts expert-level briefings on national security issues for Subscriber+Members that help provide context around today's national security issues and what they mean for business. Upgrade your status to Subscriber+ today.

During that same conference, former Assistant Secretary of Homeland Security for Cyber, Infrastructure, Risk and Resilience Policy, Matt Hayden, who also serves as a Cyber Initiatives Group Principal, noted that "anytime you do something good, the next question is what can you do more?"

"What's next? How do you improve upon the situation?" Hayden asked Wales during the summit.

"Removing the noise," Wales responded. "By that I mean the more that companies are on top of their game patching their networks and making sure that there are not vulnerable devices … [the] less notifications that we have to do."

"Second," he added, "is if you have insights … bring them to us. Our goal is try to action these as many as possible … [with] companies who have these insights, [and] who know that we're not just going to take this information and sit on it. We are going to action it as quickly as possible to make sure that these impacts don't happen."

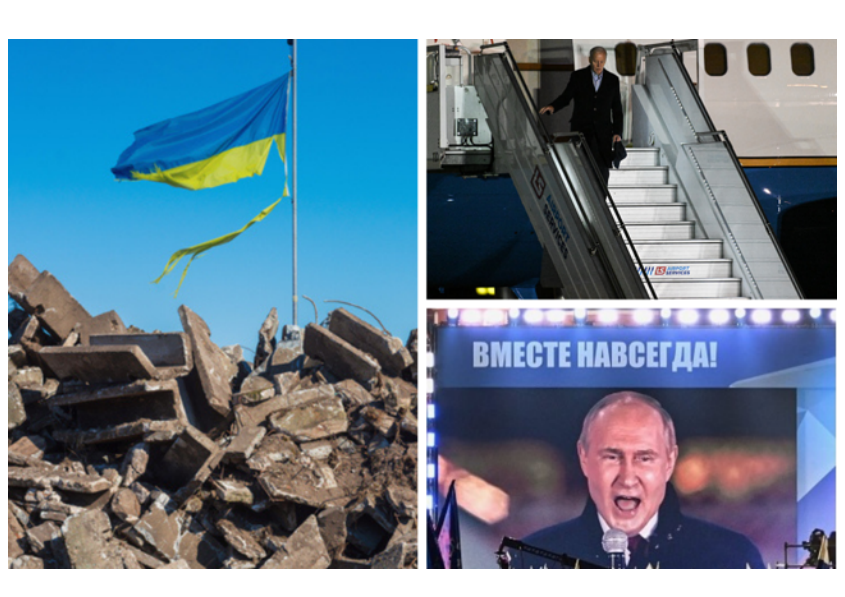
"The more insights we have in terms of the organizations being targeted," Wales added, "the more we can work upstream with our industry partners to identify other potential victims and notify them before the ransomware crew takes action."

Read more expert-driven national security insights, perspectives and analysis in The Cipher Brief because National Security is Everyone's Business

CATEGORIZED AS: CYBER

TAGGED WITH: CHINA CYBERSECURITY TECHNOLOGY

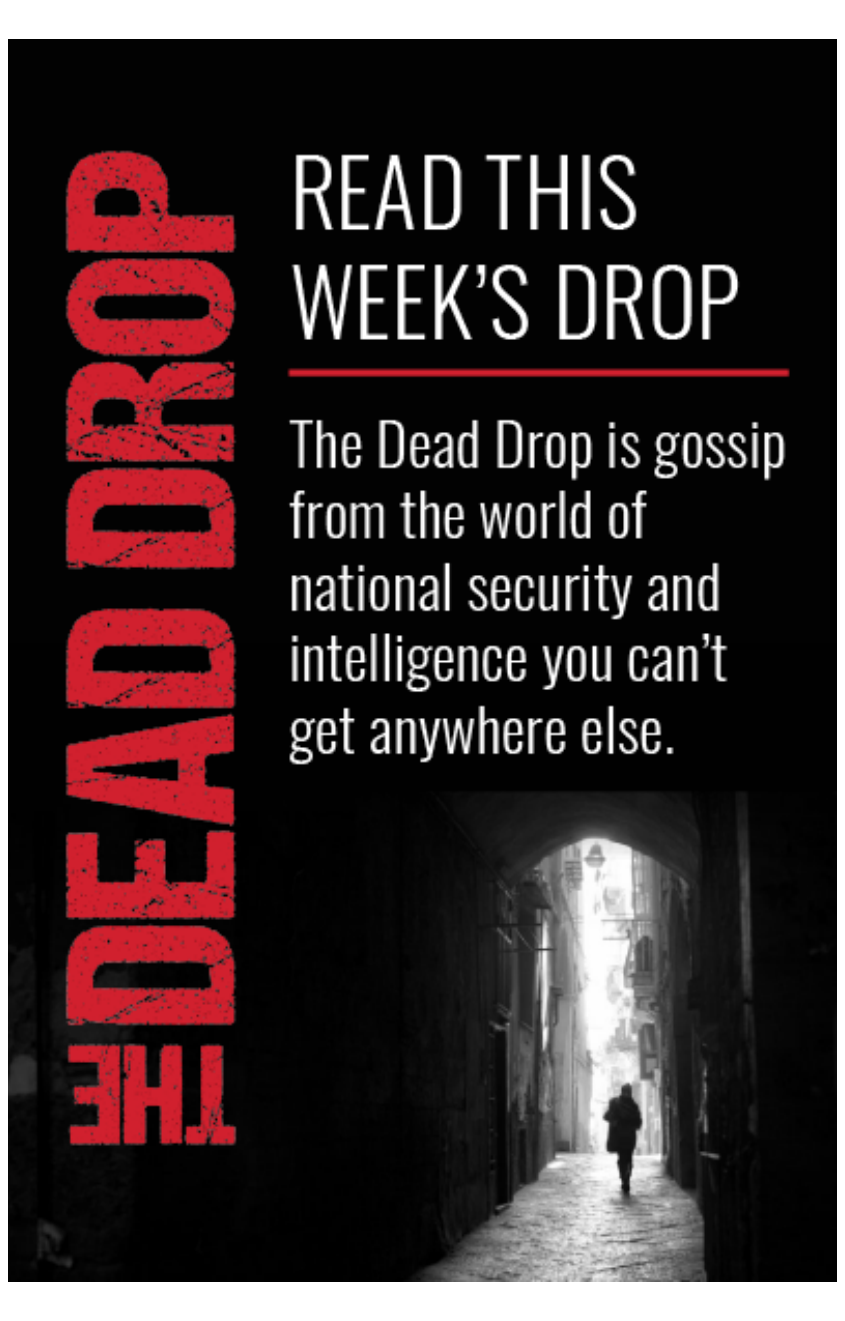
Featured Piece



Warning Signs of a More Dangerous Global Conflict

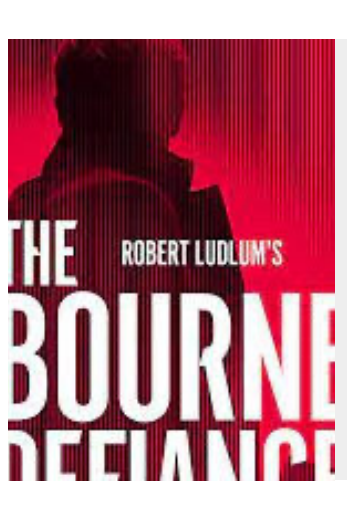
BOTTOM LINE UP FRONT — If President Joe Biden's recent remarks in Poland and President Vladimir Putin's in Moscow just a day later are any indication of the path forward, the February 24 anniversary of the Russian invasion of Ukraine may represent the beginning of a new and potentially much more dangerous phase of the conflict, which is increasingly looking like a conflict between NATO and the Russian Federation.

FEB 22, 2023, BY ROB DANNENBERG



Book Reviews

View all ›



Defiance: The Latest in The Bourne Series

BOOK REVIEW: Robert Ludlum's The Bourne Defiance By Brian Freeman / G.P. Putnam's Sons Reviewed by Elizabeth C. MacKenzie Biedell The Reviewer: Elizabeth MacKenzie Biedell […] More ›

JULY 25TH, 2023 BY THE BOURNE DEFIANCE

What the Experts Say

rief's Open
t is an
product and
daily read
l awareness
ecurity

eral John R.
n (Ret.)
ner
mander of the
O
rnational
rity Assistance

I'm proud to
network of ex
Cipher Brief,
provides supe
geopolitical a
intelligence i

Adr
Stav
Forr
Allie
NAT

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

SUBMIT COMMENT

Related Articles

MEMBERS ONLY

The Path to 2024's Election Is Engulfed With Novel Threats

CIPHER BRIEF REPORTING — The former head of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) could scarcely be more clear in his evaluations of […] More ›

ELECTION TECH/CYBER UNITED STATES

JULY 17TH, 2023 BY THE CIPHER BRIEF

MEMBERS ONLY

What is China's Volt Typhoon? And How Can It Be Stopped?

BOTTOM LINE UP FRONT – A stealthy Chinese-sponsored hacking group that blends into normal home office networks and has been pursuing efforts to disrupt critical infrastructure […] More ›

CHINA CYBER CYBER INITIATIVES GROUP TECH/CYBER

JULY 4TH, 2023

MEMBERS ONLY

When It Comes to US-China Talks, Something "Vital" Is Still Missing

CIPHER BRIEF REPORTING — A rare series of diplomatic overtures in Beijing were absent at least one "absolutely vital" ingredient, U.S. Secretary of State Antony […] More ›

CHINA CYBER CYBER INITIATIVES GROUP

JUNE 19TH, 2023 BY DAVID ARIOSTO