

# CIS Publishes Ideas to Address Real-World Threats Nationwide Amid Rising Cybersecurity Concerns

*National framework aims to better identify and prevent online and real-world threats*

EAST GREENBUSH, NEW YORK, UNITED STATES, June 27, 2024

/EINPresswire.com/ -- [Cyber attacks](#)

against U.S. critical infrastructure,

[Russian interference](#) in U.S. elections, antisemitic attacks in Michigan and New York, or AI-enabled scams: these are known as “multidimensional threats,” which often begin online but have real world implications of disruption and even violence. There is an urgent need for guidance in navigating this evolving threat landscape.

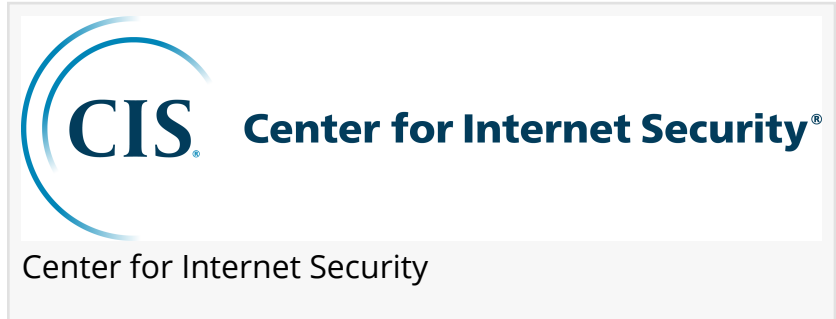
National security and cybersecurity experts at the Center for Internet Security, Inc. (CIS®) have just released “[Enhancing Safety in the Connected World: A National Framework for Action](#)” that provides law enforcement and security professionals with specific recommendations to identify and prevent multidimensional attacks, or those comprised of both cyber and physical components.

Recommendations include:

- Establishing an online threat clearinghouse infrastructure
- Better information sharing about emerging threats
- Public-private partnerships to expand awareness and build resilience
- Empowering and supporting local communities to prevent criminal activity and violence inspired by online activity

Cyberspace is no longer separate and distinct from the physical world. The two are deeply interconnected, and the way to protect them must move beyond the tactics and techniques of the past.

“This framework will provide greater insight into how those who wish to harm our society have embraced the power of the internet, and what more we can do — whether it's a government



organization, nonprofit organization, or members of the community — in order to be more resilient and better prepared to address the threat," said John Cohen, CIS Executive Director, Program for Countering Hybrid Threats.

To speak with John Cohen about how multidimensional threats are targeting local, state, and federal organizations and what needs to be done to prevent them, please contact [kelly.wyland@cisecurity.org](mailto:kelly.wyland@cisecurity.org) or call/text 518-256-6978.

###

About CIS:

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit [cisecurity.org](https://cisecurity.org) or follow us on X: @CISecurity.

Kelly Wyland

Center for Internet Security

+1 5182566978

[email us here](#)

Visit us on social media:

[Facebook](#)

[X](#)

[LinkedIn](#)

[Instagram](#)

[YouTube](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/723440700>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.