THE WHITE HOUSE
WASHINGTON

FOR IMMEDIATE RELEASE
May 13, 2021

WHAT THEY ARE SAYING:
Cybersecurity Experts, Industry Praise President Biden's Executive Order to Improve the Nation's Cybersecurity

FireEye / Mandiant: We're pleased to see this ambitious set of cybersecurity recommendations from the @WhiteHouse @POTUS and @WHNSC. We look forward to collaborating with partners in the security community and the public sector to implement the actions required by the order. [Tweet, 5/13/21]

The executive order signed by @POTUS represents crucial progress in bringing the #cybersecurity posture of the U.S. to the forefront. We applaud the @WHNSC for their work on this EO and are motivated to see these recommendations come to fruition. [Tweet, 5/13/21]

Business Roundtable: Business Roundtable applauds the White House's leadership on strengthening cybersecurity. Now is the time for the public and private sectors to work together to identify and prevent future cyber-attacks. The country is facing increasing dangers from cyberattacks, and this bold move will serve to strengthen federal government cybersecurity while using market forces to drive more transparency and more security into the software of our nation's critical infrastructure. We look forward to working with this Administration on implementation of the executive order. It is essential that we continue to build security and resilience into our businesses as we rebuild. [Statement, 5/13/21]

Amit Yoran, CEO of Tenable and founding director of US-CERT in the U.S. Department of Homeland Security: The attack on Colonial Pipeline underscores just how critical the new cyber executive order (EO) is to our national security. This is one of the most detailed and deadline-driven EOs I've seen from any administration. In the wake of a seismic attack, like SolarWinds, this is incredibly encouraging to see. Within the next year, all software vendors for the federal government must have an established software development lifecycle. While these practices won't prevent all supply chain breaches, it's an important step forward. [Statement, 5/13/21]

Matthew T. Cornelius, Executive Director of The Alliance for Digital Innovation: The Alliance for Digital applauds the Biden Administration for taking these vital, ambitious steps to improve America's cybersecurity defenses. This Executive Order highlights the critical need for government to work in close partnership and collaboration with industry leaders to identify, detect, and mitigate critical vulnerabilities, secure government information systems, and respond to growing cyber threats rapidly and effectively. ADI looks forward to working with the Administration to accelerate IT modernization, software supply chain resiliency, and the movement to zero trust architectures – all of which will be foundational to the future of public and private sector cybersecurity in the United States. [Statement, 5/13/21]

National Retail Foundation: NRF welcomes this executive order, which takes important steps to motivate software service providers to improve the security of software systems and applications that are used by the federal government. The EO will enhance the cybersecurity and resiliency of IT service providers for the retail industry and other industry sectors that rely on these same systems and applications to support their own business operations. It appropriately addresses the growing cyber risks from the software supply chain, creates strong incentives for software service providers to address these risks, and shifts away from the long-standing focus on holding the end users of software as the sole accountable party for cyber incidents. [Statement, 5/13/21]

Tom Krause, President of Broadcom Software: Broadcom applauds the White House's strategy to improve cybersecurity resiliency and to bolster the need for stronger public-private partnerships in combating cyber attacks. We look forward to working with the Administration to implement these much needed reforms. [Statement, 5/13/21]

Matt Olney, Director of Talos Threat Intelligence and Interdiction at Cisco: President Biden's Executive Order on Improving the Nation's Cybersecurity represents an aggressive and far-reaching response to some of the most challenging cybersecurity problems we face. The evolving capabilities of adversaries targeting governments and critical infrastructure have pushed defensive thinking beyond passive monitoring, password management, and perimeter firewalls. By adopting aggressive threat hunting, zero-trust architectures, and mandatory multi-factor authentication, this Executive Order is a critical step forward. We still need more aggressive engagement against those adversaries that threaten critical infrastructure, and we hope that approaches such as those recommended by the Ransomware Task Force will be adopted to pair with the changes highlighted in the executive order. From Cisco's vantage point, as a provider of critical software and an industry leader in security software, research and incident response, we stand ready as always to partner with the federal government in its efforts to secure its systems. [Statement, 5/13/21]

Bill Wright, Senior Director of Government Affairs at Splunk Inc.: The EO is taking the right approach — bold federal action coupled with private sector engagement. It's an honest, hard look at the cyber challenges that the Federal government and private sector are facing. I'm especially encouraged by the Biden administration's attempt to accelerate the adoption of Zero Trust across federal networks. [Statement, 5/13/21]

###