Expert Takeaways from the National Cybersecurity Strategy

President Biden released his National Cybersecurity Strategy, paving the way for how the White House will approach cybersecurity by aiming "to better secure cyberspace and ensure the United States is in the strongest possible position to realize all the benefits and potential of our digital future."[1] The Strategy presents five pillars and corresponding strategic objectives. The implications of this framework extend beyond America's borders and will force organizations to reevaluate their cybersecurity programs and policies. In response, experts from the FTI Cybersecurity and FTI Cybersecurity and Data Privacy Communications teams share their thoughts.

Anthony J. Ferrante, Global Head of Cybersecurity and former Cyber Incident Response Director at the National Security Council

President Biden's new strategy suggests that the best defense is a good offense. While private companies and government agencies alike possess unique insights into what our adversaries are up to in cyber space, this information has largely been used to inform a defensive posture. We know who the bad guys are and what they are doing, which can help with ensuring adequate protections are in place, but these security measures are not preventing cyber attacks from happening in the first place. With this new strategy, the U.S. is no longer going to sit flatfooted but instead leverage this intel to go on the offensive and take threat actors "off the street." This shift in approach may create unintended consequences, however, as a preemptive strike could lead to premature escalation, so offensive cyber measures should be carefully calculated before they are deployed.

Jordan Rae Kelly, Head of Cybersecurity, Americas and former Cyber Incident Response Director at the National Security Council

Cybersecurity may be one of the few issues that is not inherently politically charged. There is consensus across parties and administrations that we have needed and continue to need real change to address the significant cybersecurity risk that we face in the United States. In reviewing the new strategy, there is obvious continuity between the objectives of this policy and those of previous administrations. In fact, the authors were generous enough to say that this strategy continues the momentum of many of the priorities of the 2018 National Cyber Strategy.

First, there remains a clearly defined focus on our nation's critical infrastructure, with a recognition that there is more to do. The push from the strategy to establish more cybersecurity regulation for critical infrastructure recognizes that the previous attempts to drive voluntary compliance have been inadequate.

Second, as it relates to cyber operations policy, there has been steady maturation of the U.S. offensive cyber operational approach. This maturation reflects a refinement of previous approaches and a recognition that a more overt and aggressive approach may be necessary to drive real change. The call for the National Cyber Investigative Joint Task Force (NCIJTF) to expand its capacity to coordinate takedown and disruption campaigns is a clear signal that U.S. operations in cyberspace will now be a major disruptor of malicious cyber activity.

Brian Boetig, Senior Managing Director and former Director of the National Cyber Investigative Joint Task Force

Disrupting cyber threats and dismantling the groups behind them has been the focus of U.S. efforts for some time now. We have been closely following the evolution of legislative developments enhancing existing capabilities and the realization that cybersecurity challenges cannot be solved within the walls of government agencies alone. It requires the collective efforts of corporate America, the government, and cybersecurity professionals to make a significant impact. The strategy codifies cooperation, but the execution is still in the hands of the practitioners. Offensive cyber operations have long been sought as a tool in the U.S. cybersecurity and defense arsenal, and will indeed have significant impact on some adversaries, but come with both calculated and unforeseen risks to government and the private sector.

Kelly Miller, Managing Director, FTI Cybersecurity and Data Privacy Communications

The 'victim excuse' hasn't worked for organizations hit by cyber attacks in media for years now and with their new strategy, the White House makes clear it won't work for government scrutiny as well. While the real bad guys are threat actors, organizations with poor cyber defenses can no longer expect to come out of an incident unscathed. Forward-thinking organizations will not only implement a robust cybersecurity plan in response to this posturing from the Biden Administration, but they'll also be keen to make sure they have a crisis communications plan in place that tells a good story about how they're responding to and learning from an incident.

Sara Sendek, Managing Director, FTI Cybersecurity and Data Privacy Communications

President Biden's National Cyber Strategy is an important next step to protect and defend our nation's critical infrastructure. Cybersecurity is national security. This strategy will require a great deal of collaboration between industry and government in order to be effective. The harmonization process of all these new proposals will be a key component to the success of this strategy. Organizations will be best served by taking an active role in this process now and understand what any new regulations and requirements will mean for them and prepare accordingly. One of the most important narratives to come from this strategy is that organizations will need to take on more responsibility for cybersecurity investments and preparedness to minimize their own risk. If cybersecurity is not already a top priority, that needs to change and needs to change now.

[1] "National Cybersecurity Strategy," The White House (March 1, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.