FACTSHEET: RANSOMWARE SPRINT (APRIL – MAY 2021)

OVERVIEW

On March 31, Secretary Mayorkas outlined his vision and roadmap for the Department's cybersecurity efforts in a virtual event hosted by RSA Conference, in partnership with Hampton University and the Girl Scouts of the USA. In his speech, the Secretary announced a series of 60-day sprints to operationalize his vision, to drive action in the coming year, and to raise public awareness about key cybersecurity priorities.

The Secretary's first 60-day sprint focused on ransomware. The sprint further advanced the Secretary's call for action to tackle ransomware more effectively, which he had announced during his first month in office in February.

Cognizant that most challenges require a more sustained effort than what can be accomplished within 60 days, these sprints are designed to leverage the Office of the Secretary to (1) elevate existing work to address the specific challenge, (2) remove roadblocks that have slowed down efforts, and (3) launch new initiatives and partnerships were needed.

KEY FACTS AND OUTCOMES OF THE 60-DAY RANSOMWARE SPRINT

- *February 25*: Secretary Mayorkas issues a call for action to tackle ransomware more effectively highlighting CISA's 'Reduce the Risk of Ransomware' awareness-raising campaign
- *March 31*: Secretary Mayorkas launches the Department's first 60-day cybersecurity sprint dedicated to ransomware in his address on cyber resilience
- DHS creates an internal task force with representatives from its Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Secret Service, Coast Guard, as well as policy, legal, public affairs, and Congressional experts
- *April-May*: CISA hosts several dozen virtual engagements focusing on preventing ransomware with state, local, tribal, and territorial partners, and with private sector and critical infrastructure stakeholders
- *April 7*: Secretary Mayorkas and his four counterparts in Australia, Canada, New Zealand, and the United Kingdom issue the "Five Country Ministerial Statement Regarding the Threat of Ransomware"
- *April 29*: Secretary Mayorkas delivers keynote remarks at the launch event of the report of the Ransomware Task Force, a multi-stakeholder group of experts from industry, academia, think tank, and governments.
- *May 5*: Secretary Mayorkas urges small businesses, which constitute the majority of ransomware victims, to protect themselves against ransomware at an event hosted by the U.S. Chamber of Commerce followed by a webinar with CISA and the U.S. Secret Service providing concrete advice and recommendations to the audience
- ***May 7: Colonial Pipeline gets hit by ransomware***
- *May 10*: DHS together with Treasury convene a roundtable discussion with the insurance industry to discuss the ransomware threat and opportunities for public-private collaboration
- *May 11*: Secretary Mayorkas addresses the nation from the White House podium warning of the ransomware threat and urging organizations of all sizes to take action to better protect themselves against the threat
- *May 11*: CISA and the FBI release a joint national cyber alert "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks"
- *May 13*: CISA hosts stakeholder call focusing on ransomware with over 9,000 participants
- *May 14*: CNBC releases joint op-ed by DHS Secretary Mayorkas and Secretary of Commerce, Gina Raimondo, urging the private sector to take immediate action to protect against ransomware
- *May 21*: Secretary Mayorkas addresses business leaders in an interview with the World Economic Forum
- *May 27*: DHS's Transportation Security Administration announces the issuance of a Security Directive to better protect critical companies in the pipeline sector following the ransomware attack against Colonial Pipeline
- *Beyond the sprint*: Additional activities that grew out of the sprint include a DHS partnership with the Girl Scouts of the USA, Secretary Mayorkas discussing the threat of ransomware on ABC and CNN, and the work that will continue through the new White House-led effort to tackle ransomware through a whole-of-government effort.