HOMELAND SECURITY: CYBER MISSION OVERVIEW

President Biden has made cybersecurity a top priority for the Biden-Harris Administration at all levels of government. The Department of Homeland Security and its components, namely its Cybersecurity and Infrastructure Security Agency, play a lead role in strengthening resilience across the nation and sectors, investigating malicious cyber activity, and advancing cybersecurity alongside our democratic values and principles.

The Cybersecurity and Infrastructure Security Agency (CISA) is the nation's risk advisor. It is the federal lead for civilian network defense and lead agency for the U.S.'s critical infrastructure – with the explicit role of coordinating the federal government's efforts to promote the security and resiliency across the 16 critical infrastructure sectors and national critical functions. Through collaboration and partnerships with the public and private sectors, academia, and state, local, tribal and territorial partners, CISA drives strong cybersecurity and resilience, fosters the development and use of secure technologies; and promotes best practices.

CISA also is the lead agency protecting federal civilian unclassified systems. It plays a key role in protecting the integrity of election infrastructure. And it is working with public and private partners to build a diverse and highly skilled cyber workforce for today and for the future.

The many free programs and services CISA provides are driven by its experts' comprehensive understanding of the risk environment and corresponding cybersecurity needs. These resources are made available to federal, state, local, tribal and territorial partners, as well as private sector entities, in pursuit of a whole of nation approach to protecting our collective cybersecurity and critical infrastructure. To learn more visit, www.cisa.gov/cybersecurity.

The Transportation Security Administration (TSA) is charged with securing the nation's transportation systems, to include surface transportation (such as buses and rail), aviation, and pipelines. In close coordination with CISA, TSA uses a combination of regulation and public-private partnerships to strengthen cyber resilience across these areas. This is done through a combination of cybersecurity assessments and engagements; stakeholder education; publication of cybersecurity guidance and best practices; and use of its regulatory authority to mandate appropriate and durable cybersecurity measures.

The United States Coast Guard is the nation's lead federal agency for securing and safeguarding the maritime domain. Its role as both a military, law enforcement, and regulatory agency provides broad authority to combat cyber threats and protect U.S. maritime interests both domestically and abroad. In its role managing the maritime transportation system, it promotes best practices, identifies potential cyber-related vulnerabilities, implements risk management strategies, and has in place key mechanisms for coordinating cyber incident responses.

The United States Secret Service protects against and prosecutes a range of cyber-enabled crime – with a particular focus on protecting the nation's financial infrastructure and maintaining a safe environment for the American people to conduct financial transactions. The Secret Service also investigates and prosecutes a range of cybercrime, including network intrusions, ransomware, access device fraud, point-of-sale system compromise, illicit financing operations and money laundering, ATM attacks, identity theft and use, and business email compromise. Through the agency's Cyber Fraud Task Forces (CFTF), the Secret Service brings together critical partners, to include other law enforcement agencies, prosecutors, private industry, and academia, to pursue a comprehensive response to the threat.

Immigration and Customs Enforcement – Homeland Security Investigations (ICE HSI) is a worldwide law enforcement leader in dark net and other cyber-related criminal investigations. Using its expansive law enforcement authorities, global presence, and operational agility, HSI combats transnational cybercrime threats and the criminal exploitation of the internet by investigating, disrupting, and dismantling criminal entities that are engaged in high-impact or far-reaching cybercrime.

The Office of the Chief Information Officer (OCIO) ensures strong cybersecurity practices within the Department, so it may lead by example. OCIO works with the Department's component agencies to mature the cybersecurity posture of the Department as a whole. OCIO also ensures Component agencies are able to successfully implement and abide by established cybersecurity laws, executive orders, policies and standards.

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.