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 (DHS) and its components, 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) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. The agency connects its stakeholders in industry and government to each other and to resources, analyses, and tools to help them fortify their cyber, communications, and physical security and resilience, which strengthens the cybersecurity posture of the nation.

CISA is at the center of the exchange of cyber defense information and defensive operational collaboration among the federal government, and state, local, tribal and territorial (SLTT) governments, the private sector, and international partners. The agency has two primary operational functions. First, CISA is the operational lead for federal cybersecurity, charged with protecting and defending federal civilian executive branch networks in close partnership with the Office of Management and Budget, the Office of the National Cyber Director, and federal agency Chief Information Officers and Chief Information Security Officers. Second, CISA is the national coordinator for critical infrastructure security and resilience, working with partners across government and industry to protect and defend the nation's critical infrastructure.

The Office of Policy is leading the whole of federal government effort to coordinate, deconflict, and harmonize cyber incident reporting requirements through the Cyber Incident Reporting Council. Established under the bipartisan Cyber Incident Reporting for Critical Infrastructure Act, the Council brings together federal departments and independent regulators. Through the Council, the Office of Policy is extensively engaging with private sector stakeholders to ensure that we hear from the stakeholders themselves who will benefit from streamlined reporting requirements to ensure greater quality, quantity, and timeliness.

DHS encourages all organizations to lower the threshold for sharing information and engagement with the Government in order to raise our collective resilience to cyber threats. When cyber incidents are reported quickly, it can contribute to stopping further attacks.

The Cyber Safety Review Board (CSRB), an independent public-private advisory body administered by DHS through CISA, brings together public and private sector cyber experts/leaders to review and draw lessons learned from the most significant cyber incidents. Under the leadership of the Board's Chair, DHS Under Secretary for Policy Robert Silvers, and Deputy Chair, Google VP for Security Engineering Heather Adkins, the CSRB recently published its first report on the Log4j software vulnerability. The report included 19 actionable

recommendations for the public and private sectors to work together to build a more secure software ecosystem. DHS is already leading by example to implement the recommendations, through CISA guidance and Office of the Chief Information Officer initiatives to enhance open source software security and invest in open source software maintenance.

The Transportation Security Agency (TSA) is charged with securing the nation's transportation systems, which includes aviation, intermodal and surface transportation. The network of surface transportation operators include highway and motor carriers, freight and passenger railroad carriers, pipeline owners and operators, and mass transit carriers. In close coordination with CISA, TSA uses a combination of regulation and public-private partnerships to strengthen cyber resilience across the broad transportation network. TSA's efforts include 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 enables operations at sea, in the air, on land and space by delivering effects and capabilities in and through cyberspace. It is the nation's lead federal agency for securing and safeguarding the maritime domain. In its role as a military, law enforcement, and regulatory agency, the Coast Guard has broad authority to combat cyber threats and protect U.S. maritime interests both domestically and abroad. In support of the Maritime Transportation System (MTS), the Coast Guard continually 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 investigates a range of cyber-enabled crime with a particular focus on protecting the nation's financial infrastructure. The Secret Service cybercrime mission focuses on acts that target and threaten the American financial system, such as network intrusions and ransomware, access device fraud, ATM and point-of-sale system attacks, illicit financing operations and money laundering, identity theft, social engineering scams, and business email compromises. 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. HSI's Cyber Crimes Center (C3) delivers computer-based technical services to support domestic and international investigations into cross-border crime. C3's Child Exploitation Investigations Unit (CEIU) is a powerful tool in the fight against the sexual exploitation of children; the production, advertisement and distribution of child pornography; and child sex tourism.

The Office of the Chief Information Officer (OCIO) ensures strong cybersecurity practices within DHS, so that the Department may lead by example. OCIO works with component agencies to mature the cybersecurity posture of the Department as a whole. OCIO continues to secure and strengthen the Department of Homeland Security's cybersecurity posture by implementing and managing the DHS Information Security Program and ensuring DHS' compliance with applicable federal laws, executive orders, directives, policies, and regulations.