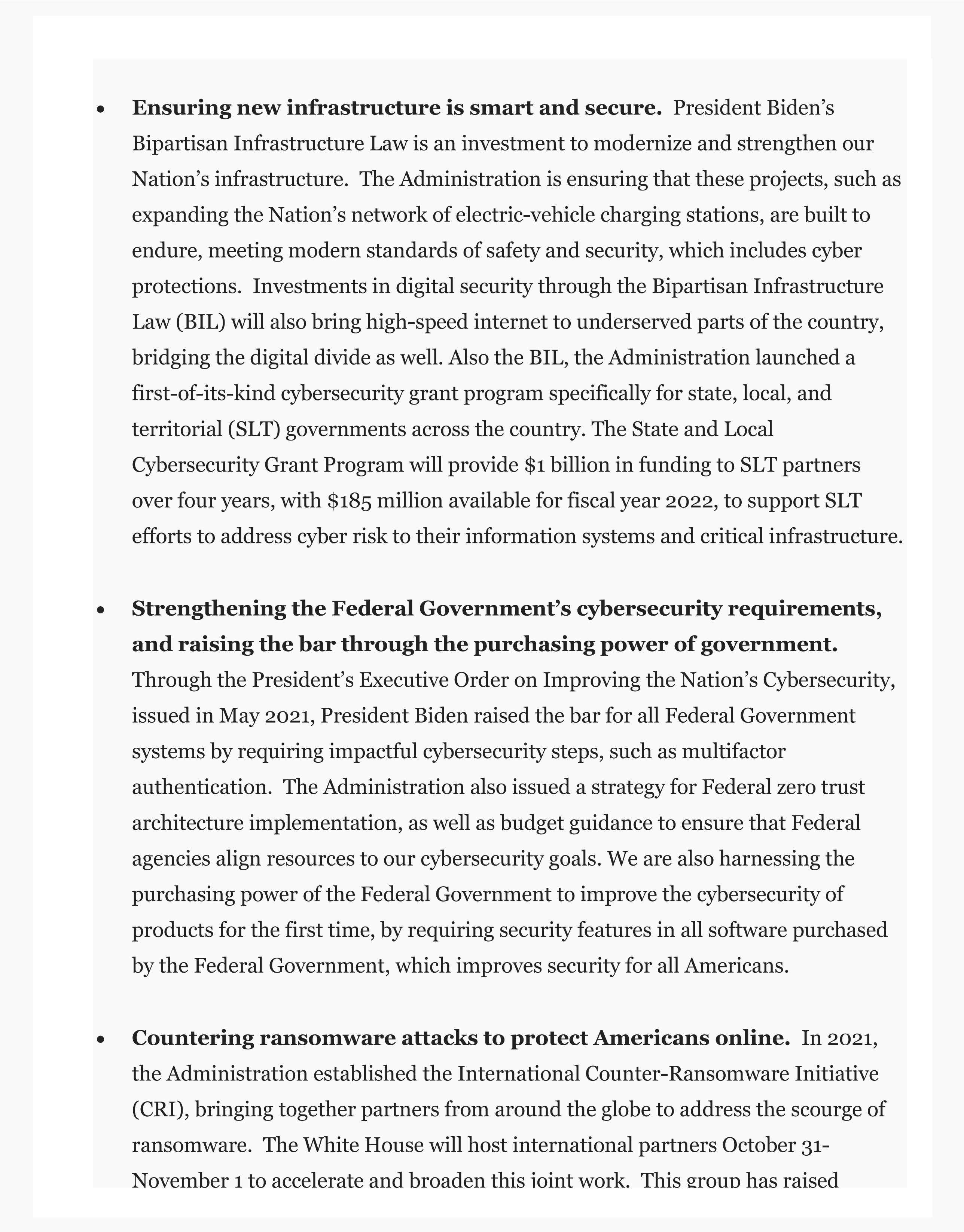
THE WHITE HOUSE
WASHINGTON

FOR IMMEDIATE RELEASE
October 11, 2022

FACT SHEET:
Biden-Harris Administration Delivers on Strengthening America's Cybersecurity

The Biden-Harris Administration has brought a relentless focus to improving the United States' cyber defenses, building a comprehensive approach to "lock our digital doors" and take aggressive action to strengthen and safeguard our nation's cybersecurity, including:

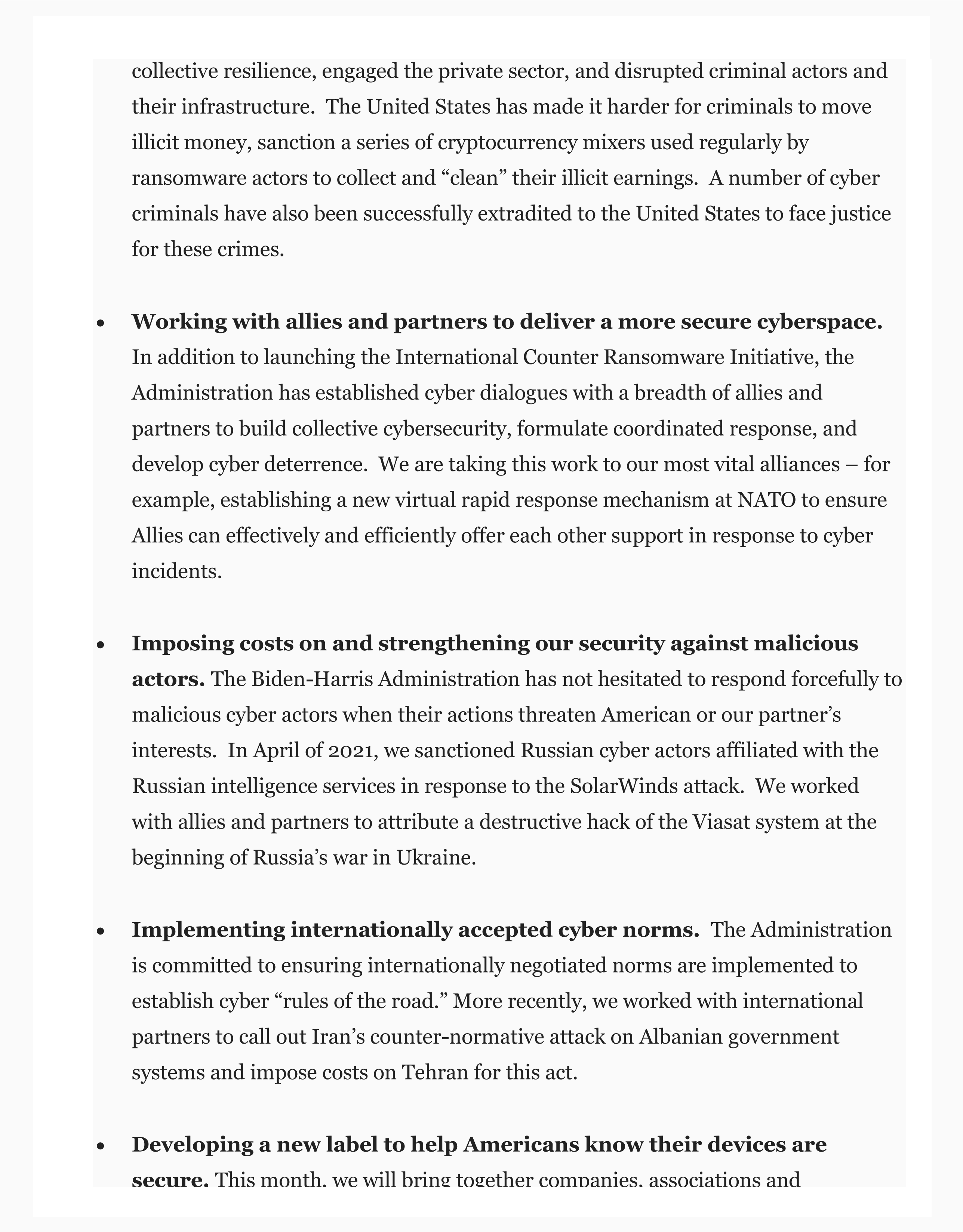
- **Improving the cybersecurity of our critical infrastructure.** Much of our Nation's critical infrastructure is owned and operated by the private sector. The Administration has worked closely with key sectors – including transportation, banking, water, and healthcare – to help stakeholders understand cyber threats to critical systems and adopt minimum cybersecurity standards. This includes the introduction of multiple performance-based directives by the Transportation Security Administration (TSA) to increase cybersecurity resilience for the pipeline and rail sectors, as well as a measure on cyber requirements for the aviation sector. Through the President's National Security Memorandum 8 on Improving Cybersecurity for Critical Infrastructure Control Systems, we are issuing cybersecurity performance goals that will provide a baseline to drive investment toward the most important security outcomes. We will continue to work with critical infrastructure owners and operators, sector by sector, to accelerate rapid cybersecurity and resilience improvements and proactive measures.



- **Ensuring new infrastructure is smart and secure.** President Biden's Bipartisan Infrastructure Law is an investment to modernize and strengthen our Nation's infrastructure. The Administration is ensuring that these projects, such as expanding the Nation's network of electric-vehicle charging stations, are built to endure, meeting modern standards of safety and security, which includes cyber protections. Investments in digital security through the Bipartisan Infrastructure Law (BIL) will also bring high-speed internet to underserved parts of the country, bridging the digital divide as well. Also the BIL, the Administration launched a first-of-its-kind cybersecurity grant program specifically for state, local, and territorial (SLT) governments across the country. The State and Local Cybersecurity Grant Program will provide $1 billion in funding to SLT partners over four years, with $185 million available for fiscal year 2022, to support SLT efforts to address cyber risk to their information systems and critical infrastructure.

- **Strengthening the Federal Government's cybersecurity requirements, and raising the bar through the purchasing power of government.** Through the President's Executive Order on Improving the Nation's Cybersecurity, issued in May 2021, President Biden raised the bar for all Federal Government systems by requiring impactful cybersecurity steps, such as multifactor authentication. The Administration also issued a strategy for Federal zero trust architecture implementation, as well as budget guidance to ensure that Federal agencies align resources to our cybersecurity goals. We are also harnessing the purchasing power of the Federal Government to improve the cybersecurity of products for the first time, by requiring security features in all software purchased by the Federal Government, which improves security for all Americans.

- **Countering ransomware attacks to protect Americans online.** In 2021, the Administration established the International Counter-Ransomware Initiative (CRI), bringing together partners from around the globe to address the scourge of ransomware. The White House will host international partners October 31-November 1 to accelerate and broaden this joint work. This group has raised



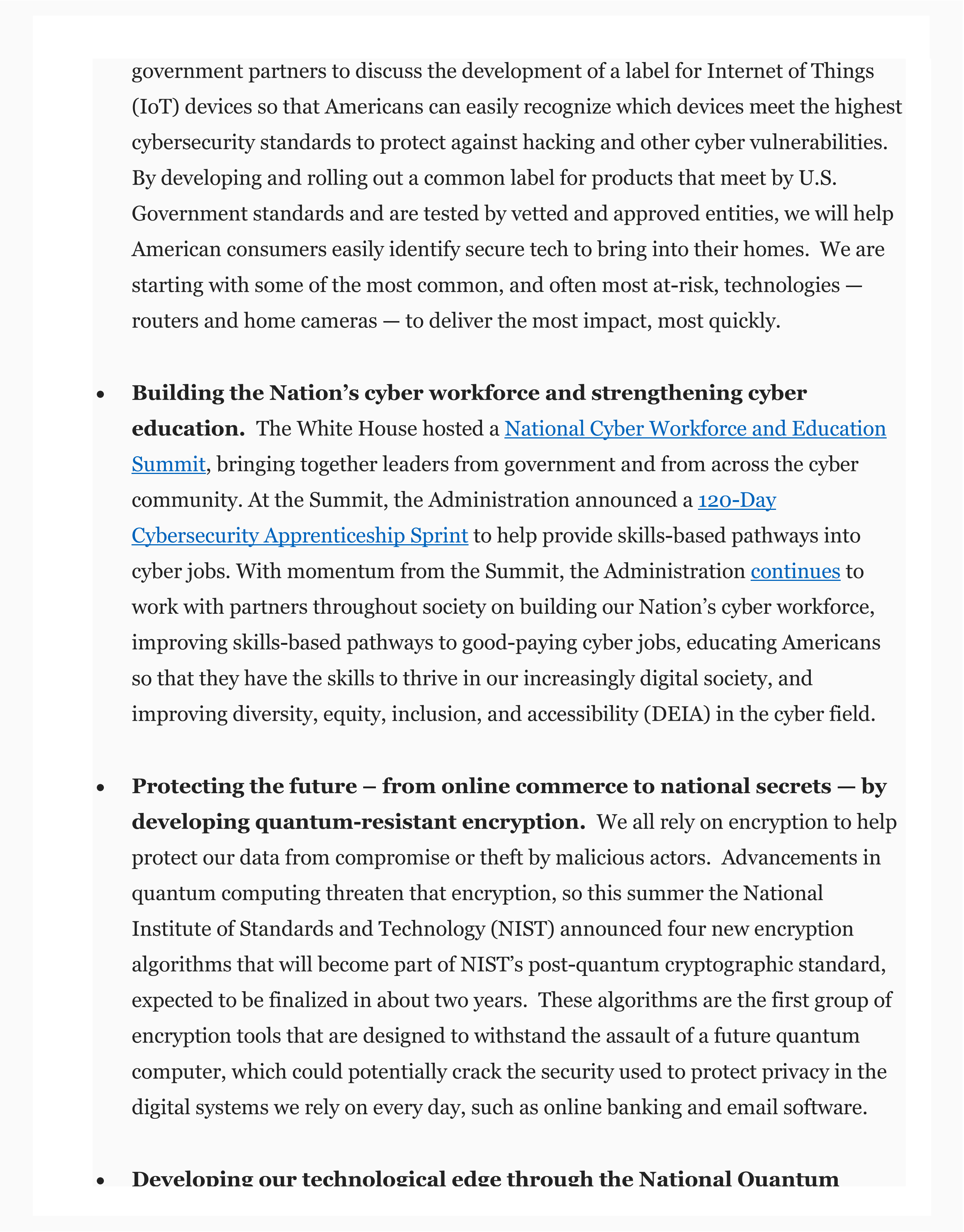
collective resilience, engaged the private sector, and disrupted criminal actors and their infrastructure. The United States has made it harder for criminals to move illicit money, sanction a series of cryptocurrency mixers used regularly by ransomware actors to collect and "clean" their illicit earnings. A number of cyber criminals have also been successfully extradited to the United States to face justice for these crimes.

- **Working with allies and partners to deliver a more secure cyberspace.** In addition to launching the International Counter Ransomware Initiative, the Administration has established cyber dialogues with a breadth of allies and partners to build collective cybersecurity, formulate coordinated response, and develop cyber deterrence. We are taking this work to our most vital alliances – for example, establishing a new virtual rapid response mechanism at NATO to ensure Allies can effectively and efficiently offer each other support in response to cyber incidents.

- **Imposing costs on and strengthening our security against malicious actors.** The Biden-Harris Administration has not hesitated to respond forcefully to malicious cyber actors when their actions threaten American or our partner's interests. In April of 2021, we sanctioned Russian cyber actors affiliated with the Russian intelligence services in response to the SolarWinds attack. We worked with allies and partners to attribute a destructive hack of the Viasat system at the beginning of Russia's war in Ukraine.

- **Implementing internationally accepted cyber norms.** The Administration is committed to ensuring internationally negotiated norms are implemented to establish cyber "rules of the road." More recently, we worked with international partners to call out Iran's counter-normative attack on Albanian government systems and impose costs on Tehran for this act.

- **Developing a new label to help Americans know their devices are secure.** This month, we will bring together companies, associations and



government partners to discuss the development of a label for Internet of Things (IoT) devices so that Americans can easily recognize which devices meet the highest cybersecurity standards to protect against hacking and other cyber vulnerabilities. By developing and rolling out a common label for products that meet by U.S. Government standards and are tested by vetted and approved entities, we will help American consumers easily identify secure tech to bring into their homes. We are starting with some of the most common, and often most at-risk, technologies — routers and home cameras — to deliver the most impact, most quickly.

- **Building the Nation's cyber workforce and strengthening cyber education.** The White House hosted a National Cyber Workforce and Education Summit, bringing together leaders from government and from across the cyber community. At the Summit, the Administration announced a 120-Day Cybersecurity Apprenticeship Sprint to help provide skills-based pathways into cyber jobs. With momentum from the Summit, the Administration continues to work with partners throughout society on building our Nation's cyber workforce, improving skills-based pathways to good-paying cyber jobs, educating Americans so that they have the skills to thrive in our increasingly digital society, and improving diversity, equity, inclusion, and accessibility (DEIA) in the cyber field.

- **Protecting the future – from online commerce to national secrets — by developing quantum-resistant encryption.** We all rely on encryption to help protect our data from compromise or theft by malicious actors. Advancements in quantum computing threaten that encryption, so this summer the National Institute of Standards and Technology (NIST) announced four new encryption algorithms that will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years. These algorithms are the first group of encryption tools that are designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day, such as online banking and email software.

- **Developing our technological edge through the National Quantum**

Initiative and issuance of National Security Memorandum-10 (NSM-10) on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. This initiative has more than doubled the United States Government's research and development (R&D) investment in quantum technology, creating new research centers and workforce development programs across the country. NSM-10 prioritizes U.S. leadership in quantum technologies by advancing R&D efforts, forging critical partnerships, expanding the workforce, and investing in critical infrastructure; will move the Nation to quantum-resistant cryptography; and protects our investments, companies, and intellectual property as this technology develops so that the United States and our allies can benefit from this new field's advances without being harmed by those who would use it against us.

###