EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

April 15, 2021 - Volume 13, Issue 7

Treasury Sanctions Russia with Sweeping New Sanctions Authority

April 15, 2021

WASHINGTON — Today, the U.S. Department of the Treasury took multiple sanctions actions under a new Executive Order (E.O.) targeting aggressive and harmful activities by the Government of the Russian Federation. Treasury's actions include the implementation of new prohibitions on certain dealings in Russian sovereign debt, as well as targeted sanctions on technology companies that support the Russian Intelligence Services' efforts to carry out malicious cyber activities against the United States.

"The President signed this sweeping new authority to confront Russia's continued and growing malign behavior," said Treasury Secretary Janet L. Yellen. "Treasury is leveraging this new authority to impose costs on the Russian government for its unacceptable conduct, including by limiting Russia's ability to finance its activities and by targeting Russia's malicious and disruptive cyber capabilities."

NEW AUTHORITY IN RESPONSE TO RUSSIAN MALIGN ACTIVITIES

The E.O. of April 15, 2021, "Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation," elevates the U.S. government's capacity to deploy strategic and economically impactful sanctions to deter and respond to Russia's destabilizing behavior.

*(*Continued On The Following Page)*

NEWSLETTER NOTES

In particular, this new E.O. authorizes sanctions to counter Russia's harmful foreign activities that threaten the national security and foreign policy of the United States, including: undermining the conduct of free and fair elections and democratic institutions in the United States and its allies and partners; engaging in and facilitating malicious cyber activities against the United States and its allies and partners that threaten the free flow of information; fostering and using transnational corruption to influence foreign governments; pursuing extraterritorial activities targeting dissidents or journalists; undermining security in countries and regions important to the United States' national security; and violating well-established principles of international law, including respect for the territorial integrity of states. To address these threats, the E.O. of April 15, 2021 authorizes sanctions on a wide range of persons, including, among others, those operating in the technology and defense and related materiel sectors of the Russian Federation economy, and in any additional sectors of the Russian Federation economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State.

SOVEREIGN DEBT PROHIBITIONS

Pursuant to the E.O. of April 15, 2021, Treasury's Office of Foreign Assets Control (OFAC) is issuing a directive that generally prohibits U.S. financial institutions from participating in the primary market for ruble or non-ruble denominated bonds issued after June 14, 2021 by the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation, and further prohibits U.S. financial institutions from lending ruble or non-ruble denominated funds to these three entities. This directive expands upon existing prohibitions on certain dealings in Russian sovereign debt that have been in place since August 2019.

TREASURY DESIGNATES RUSSIAN COMPANIES IN THE TECHNOLOGY SECTOR SUPPORTING RUSSIAN INTELLIGENCE SERVICES

Treasury's first use of the E.O. of April 15, 2021 targets companies operating in the technology sector of the Russian Federation economy that support Russian Intelligence Services. The following companies are designated for operating in the technology sector of the Russian Federation economy: ERA Technolopolis; Pasit, AO(Pasit); Federal State Autonomous Scientific Establishment Scientific Research Institute Specialized Security Computing Devices and Automation (SVA); Neobit, OOO (Neobit); Advanced System Technology, AO (AST); and Pozitiv Teknolodzhiz, AO(Positive Technologies).

*(*Continued On The Following Column)*

ERA Technopolis is a research center and technology park funded and operated by the Russian Ministry of Defense. ERA Technopolis houses and supports units of Russia's Main Intelligence Directorate (GRU) responsible for offensive cyber and information operations and leverages the personnel and expertise of the Russian technology sector to develop military and dual-use technologies.

Pasit is a Russia-based information technology (IT) company that conducted research and development in support of Russia's Foreign Intelligence Service's (SVR) malicious cyber operations.

SVA is a Russian state-owned research institute specializing in advanced systems for information security located in Russia. SVA conducted research and development in support of the SVR's malicious cyber operations.

Neobit is a Saint Petersburg, Russia-based IT security firm whose clients include the Russian Ministry of Defense, SVR, and Russia's Federal Security Service (FSB). Neobit conducted research and development in support of the cyber operations conducted by the FSB, GRU, and SVR. Neobit was also designated today pursuant to cyber-related E.O. 13694, as amended by E.O. 13757, WMD-related E.O. 13382, and the Countering America's Adversaries Through Sanctions Act (CAATSA) for providing material support to the GRU.

AST is a Russian IT security firm whose clients include the Russian Ministry of Defense, SVR, and FSB. AST provided technical support to cyber operations conducted by the FSB, GRU, and SVR. AST was also designated today pursuant to E.O. 13694, E.O. 13382, and CAATSA for providing support to the FSB.

Positive Technologies is a Russian IT security firm that supports Russian Government clients, including the FSB. Positive Technologies provides computer network security solutions to Russian businesses, foreign governments, and international companies and hosts large-scale conventions that are used as recruiting events for the FSB and GRU. Positive Technologies was also designated today pursuant to E.O. 13694, E.O. 13382, and CAATSA for providing support to the FSB.

SANCTIONS TARGET RUSSIAN MALICIOUS CYBER ACTORS

The Russian Intelligence Services — specifically the Federal Security Service (FSB), Russia's Main Intelligence Directorate (GRU), and the Foreign Intelligence Service (SVR) — have executed some of the most dangerous and disruptive cyber attacks in recent history, including the SolarWinds cyber attack. The FSB and GRU were previously sanctioned in 2016, and again in 2018, for malicious cyber activity, and most recently on March 2, 2021 for activities related to the proliferation of weapons of mass destruction (WMD).

(*Continued On The Following Page)

The FSB was involved in the August 2020 poisoning of Aleksey Navalny with a chemical weapon, specifically a nerve agent known as Novichok. The GRU also engaged in activities that materially contributed to the possession, transportation, and use of Novichok related to a March 2018 poisoning in the United Kingdom.

The FSB has also used its cyber capabilities to target Russian journalists and others who openly criticize the regime, as well as U.S. government personnel and millions of private citizens around the world. To bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks and phishing campaigns.

The GRU's malign cyber activities include deployment of the NotPetya and Olympic Destroyer malware; intrusions targeting the Organization for the Prohibition of Chemical Weapons and the World Anti-Doping Agency; cyber attacks on government systems and critical infrastructure in Ukraine and the state of Georgia; and hack-and-leak operations targeting elections in the United States and France.

In addition, the Russian Intelligence Services' third arm, the SVR, is responsible for the 2020 exploit of the SolarWinds Orion platform and other information technology infrastructures. This intrusion compromised thousands of U.S. government and private sector networks. The scope and scale of this compromise combined with Russia's history of carrying out reckless and disruptive cyber operations makes it a national security concern. The SVR has put at risk the global technology supply chain by allowing malware to be installed on the machines of tens of thousands of SolarWinds' customers. Victims of the compromise include the financial sector, critical infrastructure, government networks, and many others. Further, this incident will cost businesses and consumers in the United States and worldwide millions of dollars to fully address.

Additionally, the SVR stole "red team tools," which mimic cyber attacks to help customers better protect themselves, from a U.S. cyber security company. These tools, if made public or used offensively by the SVR or other actors, would create additional opportunities for malign actors to target computer systems worldwide.

The private and state-owned companies designated today enable the Russian Intelligence Services' cyber activities. These companies provide a range of services to the FSB, GRU, and SVR, ranging from providing expertise, to developing tools and infrastructure, to facilitating malicious cyber activities.

(*Continued On The Following Column)

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person or the receipt of any contribution or provision of funds, goods, or services from any such person.

U.S. Department of Commerce Statement on Actions Taken Under ICTS Supply Chain Executive Order

ICT Supply Chain

Today, the Department of Commerce served a subpoena on a Chinese company to support the review of transactions pursuant to Executive Order 13873, Securing the Information and Communications Technology and Services (ICTS) Supply Chain. The action taken today is an important step in investigating whether the transactions involving this company meet the criteria set forth in the Executive Order.

Unrestricted acquisition or use in the United States of ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries poses a significant risk to the national security interests of the United States. The subpoena served today allows the Commerce Department to collect information that will help make a determination regarding the potential risk to the security of United States and its citizens. The Commerce Department hopes to work cooperatively with this company to conclude a thorough review.

COMMERCE BUDGET INCLUDES ENFORCEMENT INCREASE

Combating Unfair Trade PracticesTo support the Administration's aggressive approach to a global market that allows U.S. businesses to compete fairly, the Budget provides $474 million for the International Trade Administration (ITA). The Budget will help ITA's enforcement and compliance program conduct reviews of existing antidumping and countervailing duty orders to ensure the robust enforcement of our trade laws. The Budget supports the modernization of the Committee on Foreign Investment in the United States (CFIUS) to implement the Foreign Investment Risk Review Modernization Act (FIRRMA). The Budget also provides $137.7 million for the Bureau of Industry and Security (BIS). This funding will augment the Bureau's efforts to curtail illegal exports of sensitive products and technologies while facilitating secure trade with U.S. allies and close partners. The Budget continues to support the investigations under Section 232 of the Trade Expansion Act of 1962 and includes resources to ensure timely review of exclusion requests from Section 232 trade actions.

Trans-Atlantic Dialogues II: Teaching the Holocaust in Challenging Times

Teachers and community educators from 32 countries gathered virtually March 18 for the U.S. Department of State's second in a series of international webinars on Holocaust education. The session, entitled "Trans-Atlantic Dialogues II: Teaching the Holocaust in Challenging Times," was hosted by U.S. Special Envoy for Holocaust Issues Cherrie Daniels in cooperation with the United States Holocaust Memorial Museum (USHMM).The U.S. has a longstanding commitment to promoting historically accurate Holocaust education. And our ability to do that at home took a big step forward last June in 2020, by the signing into law of the bipartisan Never Again Education Act. Allow me to share with you just one short excerpt, a very meaningful one, from that piece of legislation. It said, "As intolerance, anti-Semitism, and bigotry are promoted by hate groups, Holocaust education provides a context in which to learn about the danger of what can happen when hate goes unchallenged and there is indifference in the face of oppression of others; learning how and why the Holocaust happened is an important component of the education of citizens of the United States," close quote.

The recorded webinar with closed captioning is now available for on-demand viewing by the public at
A Webinar Hosted by the Office of the Special Envoy for Holocaust Issues
Washington, DC
https://www.state.gov/trans-atlantic-dialogue-ii-teaching-the-holocaust-in-challenging-times/

Commerce Adds Seven Chinese Supercomputing Entities to Entity List for their Support to China's Military Modernization, and Other Destabilizing Efforts

FOR IMMEDIATE RELEASE
Thursday, April 8, 2021
Office of Public Affairs

The Department of Commerce's Bureau of Industry and Security (BIS) has added seven Chinese supercomputing entities to the Entity List for conducting activities that are contrary to the national security or foreign policy interests of the United States. Today's final rule adds the following entities to the Entity List: Tianjin Phytium Information Technology, Shanghai High-Performance Integrated Circuit Design Center, Sunway Microelectronics, the National Supercomputing Center Jinan, the National Supercomputing Center Shenzhen, the National Supercomputing Center Wuxi, and the National Supercomputing Center Zhengzhou. These entities are involved with building supercomputers used by China's military actors, its destabilizing military modernization efforts, and/or weapons of mass destruction (WMD) programs.

U.S. Secretary of Commerce Gina M. Raimondo released the following statement:

"Supercomputing capabilities are vital for the development of many – perhaps almost all – modern weapons and national security systems, such as nuclear weapons and hypersonic weapons. The Department of Commerce will use the full extent of its authorities to prevent China from leveraging U.S. technologies to support these destabilizing military modernization efforts."

These entities meet the criteria for inclusion on the Entity List listed under Section 744.11 of the Export Administration Regulations (EAR).

The full list of entities impacted by this change is included in the rule on public display in the Federal Register.

The Entity List is a tool utilized by BIS to restrict the export, re-export, and in-country transfer of items subject to the EAR to persons (individuals, organizations, companies) reasonably believed to be involved, have been involved, or pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States. Additional license requirements apply to exports, re-exports, and in-country transfers of items subject to the EAR to listed entities, and the availability of most license exceptions is limited.

For more information, visit www.bis.doc.gov .

U.S. officials from Departments of Energy, State, and Commerce celebrate 10 years of Malaysia's strategic trade management

Anniversary event highlights strong U.S.-Malaysia partnership and the country's role as a regional champion of strategic trade controls

WASHINGTON – Senior U.S. officials from the Department of Energy's National Nuclear Security Administration (DOE/NNSA), Department of State's Office of the Under Secretary for Arms Control and International Security, and the Department of Commerce's Bureau of Industry and Security participated virtually in the Strategic Trade Act 10th Anniversary Celebration and Conference on April 8 and 9 to commemorate the 10th anniversary of Malaysia's commitment to implementing strategic trade controls.

The event, which garnered in-person participation by senior Malaysian officials, business leaders, several ambassadors, and an estimated 1,000 virtual attendees, highlighted the importance of strategic trade controls both in combating the proliferation of weapons of mass destruction and promoting trade facilitation.

"Export controls represent one tool to prevent the acquisition and exploitation of strategic goods that pose a threat to global security," said C.S. Eliot Kang, Senior Official for Arms Control and International Security, when opening an "Around the World" panel discussion comprised of senior nonproliferation officials from six countries. "The Strategic Trade Act's passage marked a key milestone not just for Malaysia, but also for the development of United Nations Security Council Resolution 1540-related nonproliferation policies and counter-proliferation capabilities across South East Asia."

"Malaysia's success in ensuring skilled technical experts are involved in implementing strategic trade controls helps promote secure trade and prevent the proliferation of weapons of mass destruction," said DOE Acting Under Secretary for Nuclear Security and NNSA Administrator Dr. Charles Verdon, "We are proud of our continued partnership."

"Malaysia's Strategic Trade Act has provided a strong regulatory framework for a whole-ofgovernment approach to strategic trade control administration and enforcement," said Jeremy Pelter, Acting Under Secretary for the Bureau of Industry and Security. "This innovative approach enables a robust partnership between government and industry."

*(*Continued On The Following Column)*

U.S. Ambassador to Malaysia Brian McFeeters said: "U.S.-Malaysian cooperation on strategic trade controls is an example of our enduring and comprehensive partnership on a range of issues, from expanding trade and investment opportunities to strengthening international security, nonproliferation, and countering terrorism. We are proud to work together with Malaysia as a trusted trading partner."

The U.S. Departments of Energy, State, and Commerce jointly collaborated with the Government of Malaysia for more than 15 years to share best practices on effectively managing the flow of proliferation-sensitive goods and technologies. Together, this bilateral relationship remains committed to advancing strategic trade control cooperation now and into the future.

Prepared by: Kate Hewitt, NA-PA
Caterina Fox, NA-242, 202-329-4416
Clearances: NA-EA/ Howard Dickenson
NA-20/ via Kevin Uitvlugt
NA-70/ Classification Distro
State PA/Sandra Wynn
Commerce PA/Katelyn Christ
Embassy PA/Michele Kevern

State Dept. Asks Visa Seekers Denied By Trump To Reapply

Law360 (April 2, 2021, 3:11 PM EDT) — The Biden administration invited foreign nationals seeking to work in the United States in specialty occupations, as fashion models or on landscaping sites to reapply for temporary visas after a Trump-era immigration ban expired earlier this week.

In a notice Thursday, the U.S. Department of State said foreigners who were denied H-1B, H-2B, J and L temporary visas — which cover various categories of work including scientific research, defense-related assignments and landscaping jobs — under former President Donald Trump's June 2020 proclamation would be allowed to reapply.

Executive Order on the Termination of Emergency With Respect to the International Criminal Court

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, find that, although the United States continues to object to the International Criminal Court's (ICC) assertions of jurisdiction over personnel of such non-States Parties as the United States and its allies absent their consent or referral by the United Nations Security Council and will vigorously protect current and former United States personnel from any attempts to exercise such jurisdiction, the threat and imposition of financial sanctions against the Court, its personnel, and those who assist it are not an effective or appropriate strategy for addressing the United States' concerns with the ICC. Accordingly, I hereby terminate the national emergency declared in Executive Order 13928 of June 11, 2020 (Blocking Property of Certain Persons Associated With the International Criminal Court), and revoke that order, and further order:
Section 1. In light of the revocation of Executive Order 13928, the suspension of entry as immigrants and nonimmigrants of individuals meeting the criteria set forth in section 1(a) of that order will no longer be in effect as of the date of this order and such individuals will no longer be
treated as persons covered by Presidential Proclamation 8693 of July 24, 2011 (Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions).

Sec. 2. Pursuant to section 202(a) of the NEA (50 U.S.C. 1622(a)), termination of the national emergency declared in Executive Order 13928 shall not affect any action taken or proceeding pending not finally concluded or determined as of the date of this order, any action or proceeding based on any act committed prior to the date of this order, or any rights or duties that matured or penalties that were incurred prior to the date of this order.

Sec. 3. (a) Nothing in this order shall be construed to impair or otherwise affect: (i) the authority granted by law to an executive department or agency, or the head thereof; or (ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

*(*Continued On The Following Column)*

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. (c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.
THE WHITE HOUSE, April 1, 2021.

Hong Kong Policy Act Report

March 31, 2021

Over the past year, the People's Republic of China (PRC) has continued to dismantle Hong Kong's high degree of autonomy, in violation of its obligations under the Sino-British Joint Declaration and Hong Kong's Basic Law. In particular, the PRC government's adoption and the Hong Kong government's implementation of the National Security Law (NSL) have severely undermined the rights and freedoms of people in Hong Kong.Each year, the Department of State submits to Congress the Hong Kong Policy Act Report and accompanying certification. In conjunction with this year's report, I have certified to Congress that Hong Kong does not warrant differential treatment under U.S. law in the same manner as U.S. laws were applied to Hong Kong before July 1, 1997.

This report documents many of the actions the PRC and Hong Kong governments have taken against Hong Kong's promised high degree of autonomy, freedoms, and democratic institutions. These include the arbitrary arrests and politically-motivated prosecutions of opposition politicians, activists, and peaceful protesters under the NSL and other legislation; the postponement of Legislative Council elections; pressure on judicial independence and academic and press freedoms; and a de facto ban on public demonstrations.

I am committed to continuing to work with Congress and our allies and partners around the world to stand with people in Hong Kong against the PRC's egregious policies and actions. As demonstrated by the March 16 Hong Kong Autonomy Act update, which listed 24 PRC and Hong Kong officials whose actions reduced Hong Kong's autonomy, we will impose consequences for these actions. We will continue to call on the PRC to abide by its international obligations and commitments; to cease its dismantlement of Hong Kong's democratic institutions, autonomy, and rule of law; to release immediately and drop all charges against individuals unjustly detained in Hong Kong; and to respect the human rights of all individuals in Hong Kong.

Myanmar: 'We are in danger of seeing a civil war'

Myanmar: 'We are in danger of seeing a civil war'

The ongoing unrest in Myanmar is in danger of spiralling into an "all-out civil war", a human rights group has warned.

Hundreds of people, including children, have been killed since the military seized power in February. The coup triggered mass protests that have been met with a violent response from the authorities.

"The military regime has lost control of the civil service, the population, the economy. They are in a state of panic and in doing so they have ramped up violence," Debbie Stothard, the co-ordinator of the Alternative ASEAN Network on Burma, told BBC World News.

"We are in severe danger of seeing an all-out civil war happening throughout the country," she added.

Wireless, Internet shut down in Myanmar.

Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience

Release Date:
March 31, 2021
On March 31, Secretary Mayorkas outlined his vision and roadmap for the Department's cybersecurity efforts in a virtual address hosted by RSA Conference, in partnership with Hampton University and the Girl Scouts of the USA. His prepared remarks are below:

Good morning. I am Alejandro Mayorkas, Secretary of Homeland Security. It is an honor to be here with you today.

Thank you, Professor, for the kind introduction. I am thankful that Hampton University, a historically Black university and recognized Center of Excellence in cybersecurity, has joined us for today's event. My thanks to the RSA Conference and the Girl Scouts as well, for partnering with us today.

I want to especially commend the Girl Scouts for its program in awarding cybersecurity badges to girls and young women. The program speaks proudly and strongly to our future of greater cybersecurity. It also speaks more profoundly of a better future altogether.

*(*Continued On The Following Column)*

Today is the last day of women's history month, and the words of the Girl Scouts' then-CEO, the architect of the cyber badge program, speak especially powerfully now and about the subject of our event: "We don't lead through fear. We are raising girls to be courageous, confident people. We're giving them the skills to be fearless."

Partnering with the Girl Scouts, RSA Conference, and Hampton University is exactly the type of alliance we need to achieve cybersecurity resilience.

Before I share with you my vision for the Department's cybersecurity work moving forward, allow me to share several hard truths.

First, the government does not have the capacity to achieve our nation's cyber resilience alone. So much of our critical infrastructure is in the private sector's hands. We need to work with the private sector to protect the interests of the American people and the services on which we rely. We need organizations like the Girl Scouts and Hampton University to inspire and mobilize the next generation of diverse talent to help us tackle what remains a monumental challenge.

Second, our government got hacked last year and we didn't know about it for months. It wasn't until one of the world's best cybersecurity companies got hacked itself and alerted the government, that we found out. This incident is one of many that underscores a need for the federal government to modernize cybersecurity defenses and deepen our partnerships.

Third, the government seeks to speak with one voice but too often we speak through different channels, which can confuse and distract those who need to act on our information and act fast.

We must confront these realities to develop a vision that allows us to overcome the challenges and improve our cyber resilience.

Allow me to outline the principles that will guide our work in this area moving forward, my vision for the Department as we work to realize the Biden-Harris Administration's cybersecurity strategy, and the road map for how we plan to operationalize it.

Five principles are foundational for how we think about our work.

To start, we cannot ignore the broader geopolitical context and democratic backsliding that is happening around the world. Far too often, cybersecurity is used as a pretext to infringe on civil liberties and human rights.

*(*Continued On The Following Page)*

Make no mistake: a free and secure cyberspace is possible, and we will champion this vision with our words and our actions. At the end of the day, cybersecurity is about people. It is about protecting our way of life and protecting what we hold dear.

Second, we must fundamentally shift our mindset and acknowledge that defense must go hand in hand with resilience. Bold and immediate innovations, wide-scale investments, and raising the bar of essential cyber hygiene are urgently needed to improve our cyber defenses. We need to prioritize investments inside and outside of government accordingly.

At the same time, I promised hard truths and one hard truth is that no one is immune from cyber attacks, including the federal government or our most advanced technology companies. While one can reduce the frequency of incidents through modernized defenses, ultimately it is not a question of if you get hacked, but rather when. We must therefore also bolster our capacity to respond when incidents do happen.

To advance the federal government's ability to prevent and respond to cyber incidents, the Administration is working on nearly a dozen actions for an upcoming Executive Order. More details will be shared soon. The U.S. government will improve in the areas of detection, information sharing, modernizing federal cybersecurity, federal procurement, and federal incident response. The federal government must lead by example at a time when the stakes are so high.

Pursuing cyber resilience requires a third principle, namely a focus on a risk-based approach. Determining what risks to prioritize and how to allocate limited resources is crucial to maximizing the government's impact. A fact-based framework needs to guide the assessment of risk at home and abroad.

Relatedly, addressing the most important risks is a shared responsibility. We must strengthen collaboration between the private sector and government to generate the insights necessary to detect malicious cyber actors. If actionable, timely, and bidirectional information is not distributed quickly, malicious cyber actors will gain the advantage of more time to burrow into systems and inflict damage. The final principle is to integrate diversity, equity, and inclusion – or DEI – throughout every aspect of our work. Developing sound public policy requires diverse perspectives from communities that represent America. It requires the recruitment, development, and retention of diverse talent. It requires equal access to professional development opportunities to fill the current half million cyber vacancies across our country and to prevent future shortages that threaten our ability to compete.

These five principles are the foundation of my vision. At its center is the Department's Cybersecurity and Infrastructure Security Agency, or CISA as it is commonly known.

*(*Continued On The Following Column)*

President Biden has made cybersecurity a top priority for his administration. We have elevated cybersecurity with the first ever Deputy National Security Advisor for Cyber, Anne Neuberger. That role was filled on day one of this Administration. In just the first two months, the Administration has made significant strides in remediating the impact of the SolarWinds and Microsoft Exchange incidents and we continue to work urgently to make the investments necessary to effectively defend the Nation against malicious cyber activity. Deputy National Security Advisor Neuberger is coordinating a whole-of-government response to build back better and modernize our cyber defenses. We are working closely with Congress and the private sector to get this done.

We know that CISA is integral to this objective. As some have said, the government needs a quarterback on its cybersecurity team. CISA is that quarterback.

Created less than three years ago as the country's national cyber defense center, CISA has already proven its immense value. Last year, CISA protected the integrity of the 2020 election against foreign interference. The agency has also become the Nation's risk advisor and is responsible for much more.

Among my top priorities as Secretary is to strengthen CISA to execute its mission. I am particularly grateful to Congress for further empowering CISA in recent months by providing it with additional authorities and resources.

CISA, as the Nation's cyber quarterback, is well positioned to address the hard truths I outlined earlier.

The new authorities Congress provided to CISA will enable it to proactively hunt for intruders on civilian federal government networks, shortening the amount of time they remain undetected. Once detected, CISA will continue to take action and work with civilian federal agencies to minimize risk. CISA is also expanding its ability to offer shared services based on security-by-design for these agencies. This will raise the bar and make it harder for malicious hackers to gain access in the first instance.

CISA is the private sector's most trusted interlocutor and is clearly best positioned to be the tip of the spear and the front door for the U.S. government's engagement with industry on cybersecurity.

We will therefore soon launch an awareness campaign to ensure private companies – large and small – know of the resources and services CISA has to offer. We also plan to launch an expanded cybersecurity grant program to facilitate and support the adoption of those services.

(*Continued On The Following Page)

With its strong and deep network of partnerships, CISA is the ideal nexus for the government to mobilize action and advance cyber resilience across all sectors and at every level of government. CISA's role in leading national efforts to secure the 2020 election illustrates what we can accomplish through strong partnerships, a clear vision, and an appropriate sense of urgency.

Looking ahead, expanding CISA's footprint across the country will be critical to institutionalize and maximize its network of partnerships. CISA is already moving ahead with placing State Cybersecurity Coordinators across the country, deepening its longstanding relationships from coast to coast. The Department is also working on a proposal for a Cyber Response and Recovery Fund that will further augment CISA's ability to provide assistance to state, local, tribal, and territorial governments.

Of course, we know that even the best quarterback can't win a game alone. CISA fulfills its lead role for national cyber resilience in collaboration with other agencies at every level of government. This includes federal law enforcement agencies who bring cyber criminals to justice. Our Intelligence Community, which focuses on better understanding how our cyber adversaries intend to compromise American networks. And other agencies with the capability to impose costs on malicious cyber actors. This also includes the National Cyber Director – a newly created Senate-confirmed position that our Administration is committed to position for success.

Beyond CISA, the Department has other unique capabilities it brings to bear to better protect the nation against cyber threats. The U.S. Coast Guard, which is also part of DHS, plays a critical role in increasing the cyber resilience of the maritime transportation system through which 90 percent of U.S. imports and exports – worth $5.4 trillion – pass through. The Department will continue to implement the National Maritime Cybersecurity Plan released by the previous administration to enable the Coast Guard's important work in this area.

The Department will also empower the Transportation Security Administration to increase the cyber resilience of other transportation systems – from rail to pipelines – that fuel so much of our economy.

Last and certainly not least, the Department will continue to ensure the U.S. Secret Service and ICE's Homeland Security Investigations remain well positioned to combat 21st century crimes.

Let me be clear: the numbers are staggering. According to the FBI, the reported losses tied to cybercrime exceeded $4.1 billion last year alone. The Secret Service arrested more than 1,000 people for cyber-financial crimes and prevented over $2 billion in potential fraud losses.

(*Continued On The Following Column)

These numbers highlight that cybersecurity is not some abstract concept or a threat limited to the government or critical infrastructure. Hackers target American citizens directly every day and impact their lives at a time when we have experienced unprecedented hardships. Communities of color across the country are disproportionately impacted through this activity.

Many of these crimes are transnational in nature and require international cooperation to address. Fighting cybercrime more effectively therefore also reflects the Biden-Harris administration's commitment to a foreign policy for all Americans. We must align our foreign policy priorities and international partnerships accordingly.

Finally, and this applies to everything I have said so far: DHS must lead by example. We must have our own house in order before we can expect others to heed our advice. We must model what effective partnerships look like. We must ensure our own workforce is reflective of the communities we serve.

So, how will we move from vision to action?

We will proceed along two tracks.

First, I am announcing today a series of 60-day "sprints," each focused on the most important and most urgent priorities needed to achieve our goals. Second, we will focus on four medium-term priorities that will receive my sustained attention over the longer term.

The series of sprints will mobilize action by elevating existing efforts, removing roadblocks, and launching new initiatives where necessary.

Each sprint has a dedicated action plan to drive action within the Department and energize our engagement with partners in the private and public sectors, both domestically and internationally.

The first sprint will focus on the fight against ransomware, a particularly egregious type of malicious cyber activity that usually does not discriminate whom it targets. It is malicious code that infects and paralyzes computer systems until a ransom has been paid. Individuals, companies, schools, even hospitals and other critical infrastructure have been among the victims.

Let me be clear: ransomware now poses a national security threat. Last fall, CISA and its government partners issued a joint alert warning of increased ransomware attacks that could paralyze hospitals and other health care facilities. There are actors out there who maliciously use ransomware during an unprecedented and ongoing global pandemic, disrupting hospitals as hundreds of thousands die. This should shock everyone's conscience.

(*Continued On The Following Page)

Those behind these malicious activities should be held accountable for their actions. That includes governments that do not use the full extent of their authority to stop the culprits. We must condemn them for it and remind them that any responsible government must take steps to prevent or stop such activity.

We will do everything we can to prevent and respond to these horrendous acts. And we call on others around the world to do the same.

In the coming weeks, the Department will step up our efforts to tackle ransomware on both ends of the equation. With respect to preventing ransomware incidents, we will take action to minimize the risk of becoming a victim in the first place. We will launch an awareness campaign and engage with industry and key partners, like insurance companies. With respect to responding to ransomware attacks, we will strengthen our capabilities to disrupt those who launch them and the marketplaces that enable them.

Closely related to this first sprint, is the second sprint focusing on the cybersecurity workforce. We cannot tackle ransomware and the broader cybersecurity challenges without talented and dedicated people who can help protect our schools, hospitals, critical infrastructure, and communities.

During the workforce sprint, which we will launch next month, we will focus on several elements. Front and center is support for our current workforce, who have done a heroic job protecting the election and now responding to two major incidents.

In addition, we will set an example and launch a DHS Honors Program with an initial focus on cybersecurity. We will also start publishing DHS's DEI data and step up our internal DEI strategy to ensure we are attracting, developing, and retaining the best diverse talent.

Beyond DHS, we will champion DEI across the cyber workforce of the entire federal government.

To this end, I am excited that we are partnering with the Girl Scouts today and exploring additional opportunities for us to collaborate in the future. To further help inspire the next generation of diverse cyber talent, we will also expand our cybersecurity education and training program that has reached over 25,000 teachers so far. Later this summer, we will launch our third sprint focused on mobilizing action to improve the resilience of industrial control systems. The cybersecurity incident at the water treatment facility in Florida last month was a powerful reminder of the substantial risks we need to address.

*(*Continued On The Following Column)*

The last three sprints for the coming year will focus on better protecting our transportation systems, safeguarding election security, and advancing international capacity-building.

While the series of sprints will drive action over the coming year, we will also focus on several medium- to long-term priorities that will have my sustained personal attention.

First, we need to cement the resilience of our democratic infrastructures. We have made great progress to protect the integrity of elections, which we will need to continue to safeguard in the years to come. We must also improve the resilience of the other infrastructure our democracy depends upon. Several high-profile attacks against our allies and partners are warning signs that we must focus on securing all our democratic institutions, including those outside of the executive branch.

Second, following last year's supply chain compromise targeting the federal government, we must build back better. This cannot be done in a sprint, as it will take months or even years to fully implement. We are grateful to Congress for the support provided to CISA through the American Rescue Plan, which is a down payment to address this urgent challenge.

Third, the exploitation of SolarWinds highlighted that we need to think about supply chain risks holistically. While some risks are clearly associated with certain foreign companies and governments, we need a risk-based approach to ensure we address all systemic supply chain risks. Bearing in mind that 100% cybersecurity is not possible, this includes considering zero trust architectures where needed to reach the level of resilience required.

Finally, we must ensure that our work is not driven only by the crisis of the day. We must get ahead of the curve and think long term. It is imperative to dedicate senior leadership attention to strategic, on-the-horizon issues.

For example, the transition to post-quantum encryption algorithms is as much dependent on the development of such algorithms as it is on their adoption. While the former is already ongoing, planning for the latter remains in its infancy. We must prepare for it now to protect the confidentiality of data that already exists today and remains sensitive in the future.

This is a priority and DHS will start developing a plan for how it can help facilitate this transition. Considering the scale, implementation will be driven by the private sector, but the government can help ensure the transition will occur equitably, and that nobody will be left behind.

For too long, cybersecurity has been seen as a technical challenge couched in bureaucratic terms.

(*Continued On The Following Page)

But cybersecurity is not about protecting an abstract "cyberspace." Cybersecurity is about protecting the American people and the services and infrastructure on which we rely.

With over $4 billion in cybercrime losses reported to the U.S. government last year alone, it affects the wallets of Americans across the country, often the most vulnerable – elderly and unemployed individuals reliant on government assistance, communities of color, and American families. And as we have seen with the wave of ransomware attacks and intrusions into critical infrastructure, cyber threats are coming dangerously close to threatening our lives.

We need to be clear-eyed that this is also about protecting democracy at home and abroad.

For this reason, today's event is designed to outline a vision and to provide a road map. I could not imagine a more ideal group of partners to launch this call for action than the RSA Conference, Hampton University, and the Girl Scouts. I look forward to what we all can accomplish together in the months to come.

SpaceX wins NASA contract to build spacecraft to fly astronauts to the moon

The award surprised some in the space community, who expected NASA to pick two companies so it would have a backup. SpaceX beat out Blue Origin, the space venture founded by Amazon's Jeff Bezos, and Dynetics, a defense contractor based in Alabama. By going with a single provider, NASA won't have a backup if the company stumbles.

"There is no elevator to success. You have to take the stairs."

U.S. and other signatories of Iran nuclear deal plan meetings in Vienna to discuss efforts on reviving pact

Iran and world powers plan to meet Tuesday, April 6 on efforts to restore the accord to curb Tehran's nuclear program after the Trump administration pulled out and reimposed sanctions.

The talks in Vienna will include "separate contacts" between U.S. envoys and nations taking part in the meeting, including China, France, Germany, Russia, Britain and Iran, according to a European Union statement.

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)