S. HRG. 115–371

# RUSSIA SANCTIONS: CURRENT EFFECTIVENESS AND POTENTIAL FOR NEXT STEPS

## HEARING

BEFORE THE

## COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING THE IMPLEMENTATION AND EFFECTIVENESS OF THE SANCTIONS PROGRAM CURRENTLY IN PLACE AGAINST RUSSIA

AUGUST 21, 2018

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: https://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
32–576 PDF WASHINGTON : 2019

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

| | |
|---|---|
| RICHARD C. SHELBY, Alabama | SHERROD BROWN, Ohio |
| BOB CORKER, Tennessee | JACK REED, Rhode Island |
| PATRICK J. TOOMEY, Pennsylvania | ROBERT MENENDEZ, New Jersey |
| DEAN HELLER, Nevada | JON TESTER, Montana |
| TIM SCOTT, South Carolina | MARK R. WARNER, Virginia |
| BEN SASSE, Nebraska | ELIZABETH WARREN, Massachusetts |
| TOM COTTON, Arkansas | HEIDI HEITKAMP, North Dakota |
| MIKE ROUNDS, South Dakota | JOE DONNELLY, Indiana |
| DAVID PERDUE, Georgia | BRIAN SCHATZ, Hawaii |
| THOM TILLIS, North Carolina | CHRIS VAN HOLLEN, Maryland |
| JOHN KENNEDY, Louisiana | CATHERINE CORTEZ MASTO, Nevada |
| JERRY MORAN, Kansas | DOUG JONES, Alabama |

GREGG RICHARD, *Staff Director*
MARK POWDEN, *Democratic Staff Director*

JOHN O'HARA, *Chief Counsel for National Security Policy*
KRISTINE JOHNSON, *Professional Staff Member*

ELISHA TUKU, *Democratic Chief Counsel*
LAURA SWANSON, *Democratic Deputy Staff Director*
COLIN MCGINNIS, *Democratic Policy Director*

DAWN RATLIFF, *Chief Clerk*
CAMERON RICKER, *Deputy Clerk*
JAMES GUILIANO, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

# C O N T E N T S

## TUESDAY, AUGUST 21, 2018


Page

Opening statement of Chairman Crapo ..... 1
Prepared statement ..... 47
Opening statements, comments, or prepared statements of:
Senator Brown ..... 2
Prepared statement ..... 47


## WITNESSES


Sigal P. Mandelker, Under Secretary, Terrorism and Financial Intelligence, and Acting Deputy Secretary, Department of the Treasury ..... 5
Prepared statement ..... 49
Responses to written questions of:
Senator Brown ..... 77
Senator Toomey ..... 78
Senator Cotton ..... 78
Senator Menendez ..... 79
Senator Tester ..... 79
Senator Warren ..... 80
Senator Donnelly ..... 81
Senator Schatz ..... 82
Christopher Krebs, Under Secretary, National Protection and Programs Directorate, Department of Homeland Security ..... 6
Prepared statement ..... 70
Responses to written questions of:
Senator Brown ..... 83
Senator Moran ..... 84
Senator Tester ..... 88
Christopher A. Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, Department of State ..... 8
Prepared statement ..... 73
Responses to written questions of:
Senator Brown ..... 89
Senator Toomey ..... 90
Senator Cotton ..... 91
Senator Menendez ..... 92
Senator Schatz ..... 93

# RUSSIA SANCTIONS: CURRENT EFFECTIVENESS AND POTENTIAL FOR NEXT STEPS

**TUESDAY, AUGUST 21, 2018**

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
*Washington, DC.*

The Committee met at 10:02 a.m., in room SD–538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

## OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. This hearing will come to order.

This morning the Committee will receive testimony from senior Administration officials from the Departments of Treasury, State, and Homeland Security on the implementation and effectiveness of the sanctions program currently in place against Russia.

The reasons for these sanctions include Russia's standing military incursions in Ukraine; abetting Assad's atrocities in Syria; conducting cyberenabled information warfare activities and cyberattacks against United States critical infrastructure, including its malicious meddling in U.S. elections; and a host of other malign Russian activities.

The Banking Committee plays a leading role in developing any legislation that proposes the use of sanctions and financial pressure, more especially those measures involving financial institutions, sovereign debt, and other financial instruments to address serious threats to the national security of the United States.

Just about 1 year ago, on August 2nd, the President signed into law the Countering America's Adversaries Through Sanctions Act of 2017, known as "CAATSA", which included in it, among other things, authorities for not only a set of strengthened sanctions against Russia but also brand-new authorities for several powerful mandatory secondary sanctions.

It was this Committee that put together the foundation for those sanctions and financial measures on Russia and then worked with the Committee on Foreign Relations to expand them as a part of CAATSA.

CAATSA was truly a foursquare effort. It was not only strongly bipartisan but also bicameral. It passed the House by a vote of 419–3, and 2 days later by the Senate on a vote of 98–2.

It is not often that Congress acts together in such a strong manner, as marked by near-unanimous votes. But then Russia is a menace on so many different levels today that Congress can be

compelled to act with a single voice to find solutions that will protect America and democratic values across the world.

To its credit, the Administration, in the year since CAATSA, has imposed some of the toughest sanctions on Russia in years, particularly with regard to those imposed in April on Russia's oligarchs and their business associations.

The bulk of sanctions imposed against Russia pertain to its unlawful invasion and annexation of Crimea. These were strengthened by Congress in CAATSA and, absent any other change in Putin's behavior, will likely remain in place until he is no longer in power and Crimea is returned.

In all, over the last year the Administration has sanctioned over 200 targeted Russian individuals and entities, for either its cyberattacks or Ukraine behavior, either pursuant to congressional sanctions or under its own executive authority. I hope to receive an update today from our witnesses on how the sanctions against Russia are being implemented and enforced.

It was a positive step when, 2 weeks ago, in response to Russia's use of a nerve agent in Britain against one of its former spies and his daughter, the State Department showed its resolve against Moscow while it took a stand with our British allies by imposing a set of escalatory sanctions under the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991.

The Administration is taking some important steps against Putin, his cronies, and the industrial apparatus they control. But can Congress expect more from the Administration? And when?

Congress itself is positioned to do more. There are bills in this Committee and in the Foreign Relations Committee which seek to escalate economic pain throughout Russia's banking and energy sectors and sovereign debt markets.

As we all—and that includes the Administration—consider next steps to further constrain Putin, including sanctions and other diplomatic initiatives, two questions come to mind:

What degree of success have the existing evolutions of sanctions, which work to constrain the Russian economy and derail the activities of those individuals closest to Putin, had on Putin's behavior at home and abroad?

And, second, what is the most effective way to coordinate and strengthen sanctions with our European allies and other partners?

We will obviously have many more questions, but I am finished with that at this point.

Senator Brown.

**OPENING STATEMENT OF SENATOR SHERROD BROWN**

Senator BROWN. Thank you, Mr. Chairman. I am really glad you are holding this hearing. Thank you to our witnesses for serving in our Government. This is the first in the coming weeks on sanctions and other measures to more forcefully counter Russia's continuing efforts to attack the United States and our allies.

While sanctions have had some effect on Russia's economy, it is less clear what effect they have had on its malign activities around the world. Russia remains in Crimea, its proxies are still in Eastern Ukraine, it serves as the arsenal of Assad, and it continues to attack our elections and other critical infrastructure.

Earlier this morning Microsoft issued a new report outlining Russian attacks on the U.S. Senate and on think tanks, mostly anti-Russia or anti-Trump think tanks, one of which hosts an important kleptocracy initiative targeting oligarchs close to Putin. True to form, the Kremlin promptly denied involvement. That is nonsense. The President should call it that and forcefully respond.

Our Government—we and the President both—must right now send a more powerful and direct message to Putin and those within his circles: "We know what you are doing. It must stop. And if it continues, if you continue, you and your Government will pay a dear price." So far the President has basically been AWOL, undercutting even modest efforts of professionals in Treasury, in State, in DHS, and the intelligence community.

Over a year ago, Congress gave the President, as the Chairman just said, the authority to use more assertive sanctions against Russia. My colleagues and I have pressed for nearly a year for stronger CAATSA implementation. After months of waiting, we requested assessments by the Inspectors General of the intelligence community, State, and Treasury Departments.

These hearings and these IG audits are not simply a reaction to the President's startling performance in Helsinki, which was widely panned on both sides of the aisle and both sides of the Atlantic. There is a deeper problem. With a few exceptions, the President has refused to forcefully use the new authorities under CAATSA.

Let me give one example. Administration officials identified Russians responsible for supplying chemical weapons components for use in Syria, the ones that killed and maimed men, women, and children. Our U.N. Ambassador announced the imminent imposition of sanctions. The next day they were withdrawn, reportedly on orders from the President.

Instead, the Administration requested that a broader waiver to Section 231 be included in the defense bill, basically because the President could not certify the key condition of the existing waiver: that Russia was reducing its cyberattacks against the United States.

I think it was a bad idea to use the recent defense bill to relax waiver authorities on Russian defense and intelligence sector sanctions. Instead of strengthening sanctions, we have gone in the opposite direction.

That is why the Administration continues to face fierce bipartisan criticism from this Committee, from this body, on its Russia policy, why a new round of oversight hearings is being convened—and I give the Chairman credit for that—and why members on both sides are proposing new sanctions.

In addition to urging the Administration to use CAATSA more aggressively, I think most of us agree Congress should also do more to increase pressure. Congress crafted tough Russia sanctions enacted last August by overwhelming majorities in both chambers. We should build on that.

We should focus on the facts and broader strategic questions: What is Russia's Government still doing in Syria and Ukraine? What active cyberattacks are they directing against our elections and critical infrastructure? What powerful economic, trade, finan-

cial, diplomatic, and political tools can we deploy now to deter those attacks?

Russia's election interference, confirmed unanimously by U.S. intelligence earlier this year and reaffirmed again today, poses a problem that goes far beyond foreign policy and strikes at the core of our democracy. In no way is this a partisan issue.

We are 77 days away from another election, and the Director of National Intelligence, Microsoft, and others have been sounding the alarm that the warning lights are flashing red again. And while some efforts are being made to bolster State election security measures and otherwise contain these threats, it appears little is being done to address their source: Russia's Government.

I know my constituents are clear-eyed about these threats. The Ukrainian community in Ohio and around the world knows firsthand—like our NATO allies Latvia, Lithuania, Estonia—the dangers of unchecked Russian aggression.

That is why we should not only press to more aggressively implement current Russian sanctions, but we must also strengthen our response. New bipartisan sanctions measures have been introduced. These hearings are a critical next step.

Thank you to the three of you for joining us today. I am interested to hear where we are, what effects, if any, the current sanctions regime is having on Russia's economy and, more importantly, on its behavior, and your ideas on how we will more forcefully confront these threats in the months to come.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you, Senator Brown.

Today we will hear testimony from three Administration officials who deal firsthand with confronting the Russia threat.

We will first hear testimony from Ms. Sigal Mandelker, the Acting Deputy Secretary and current Under Secretary of Treasury for Terrorism and Financial Crimes, who is the country's chief sanctions architect.

Next we will hear from Mr. Christopher Krebs, the Under Secretary of Homeland Security at the National Protection and Programs Directorate, who is responsible for reducing, if not eliminating, then recovering from threats to our Nation's cyber and communications and other infrastructure.

And, finally, we will hear from Dr. Christopher Ford, the Assistant Secretary of State responsible for the Bureau of International Security and Nonproliferation at the State Department, who can provide us with some valuable insight on challenges with Russia.

As you can see, Members of the panel, we have a very good attendance, and a number of those who are not here are at a different hearing on Russia in the Foreign Relations Committee. And because of that I thank you, first of all, for your written testimony. It is extremely helpful to us. I ask you to honor and remember the 5-minute rule for your oral testimony so we can get through the questioning period from our Senators. And I also remind our Senators that we have a 5-minute rule, and we will try today to stick very closely to that.

With that, Ms. Mandelker.

**STATEMENT OF SIGAL P. MANDELKER, UNDER SECRETARY, TERRORISM AND FINANCIAL INTELLIGENCE, AND ACTING DEPUTY SECRETARY, DEPARTMENT OF THE TREASURY**

Ms. MANDELKER. Thank you. Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee, thank you for inviting me here today to speak on behalf of the Treasury Department and provide an update on our comprehensive efforts to counter Russia's malign activity. Our efforts, taken together with our partners across the U.S. Government and around the world, are guided by a clear understanding of the threat Russia poses to the United States and to our friends and allies.

As this Committee is well aware, Russia seeks to challenge the United States and its allies in a variety of ways. They are continuing their occupation of Crimea and ongoing aggression against Ukraine. They are attempting to subvert Western democracies, including our own, through election interference. They have used chemical weapons in an attempt to assassinate a British citizen and his daughter in the United Kingdom. They are perpetrating malicious cyberattacks, and they are facilitating sanctions evasion and other illicit activity across the globe. The breadth and brazenness of Russia's malign conduct demands a firm and vigorous response.

Precisely for this reason, Treasury's Russia sanctions program is among our most active and impactful. Since January 2017, this Administration has sanctioned 229 Russian-related individuals and entities for a broad range of access, 212 of which were sanctioned by there's Office of Foreign Assets Control, including a number this morning.

Indeed, we have issued Russia-related measures in 7 of the last 9 months in a number of different actions. In doing so, we have targeted a veritable "Who's Who" of Russia's most prominent companies. These include Russia's primary State-owned weapons trading company, one of the largest independent power companies in Russia, and a major Russian oil company. Our targets also include the heads of major State-owned banks and energy firms, such as VTB Bank and Gazprom, as well as some of Putin's closest associates. These figures include Putin affiliates Oleg Deripaska and Viktor Vekselberg, as well as Putin's son-in-law.

Indeed, those who deal with such persons risk being targeted by our powerful secondary sanctions authorities under CAATSA. Sanctioning these Russian individuals and entities has made them radioactive. We have made clear to the world that those who choose to continue to do business with them do at their own peril.

That CAATSA was passed by a near-unanimous vote demonstrated great resolve by Congress to counter Russia's malign activity, and we share that resolve.

As companies across the globe work to distance themselves from sanctioned Russian persons, our actions are imposing an unprecedented level of financial pressure on those supporting the Kremlin's malign agenda and on key sectors of the Russian economy, as the impacts of our Russia-related actions are felt far and wide.

Indeed, Treasury's actions have extensively impacted the financial interests of targeted individuals and entities. Our oligarch sanctions alone have substantially reduced the net worth of those

individuals and their companies. Similarly, other companies designated for their links to Crimea have been forced to cut production and have lost business relationships with foreign commercial partners.

In addition, we have cutoff malicious cyberactors from the U.S. financial system and beyond, including those providing offensive cybercapabilities to the Russian intelligence services and covertly working on behalf of the Kremlin to interfere with the 2016 U.S. election.

In addition to sanctions, we are also strategically and smartly deploying Treasury's other economic authorities to disrupt Russia's illicit financial conduct and harden the international financial system against its predation. And we regularly engage our foreign allies and partners, especially those in Europe, to coordinate these efforts and augment the impact of our sanctions and our other actions.

By strategically leveraging all of our complementary authorities, we are increasing financial pressure on Russia to advance our national security priorities while simultaneously mitigating collateral impacts on the United States, our European allies, and the global economy.

There is no question that we have imposed major costs on Russia. Yet the significance of our actions and our other financial measures must ultimately be measured in terms of their strategic impact. Though Russia's malign activities continue, its adventurism undoubtedly has been checked by the knowledge that we can bring even more economic pain to bear using our powerful range of authorities—and that we will not hesitate to do if its conduct does not demonstrably and significantly change.

Thank you.

Chairman CRAPO. Thank you.

Mr. Krebs.

**STATEMENT OF CHRISTOPHER KREBS, UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY**

Mr. KREBS. Chairman Crapo, Ranking Member Brown, Members of the Committee, thank you for the opportunity to discuss the Department of Homeland Security's ongoing efforts to mitigate cybersecurity risk to our Nation's critical infrastructure. Safeguarding and securing cyberspace is a core homeland security mission in an area that I have the honor to lead for DHS.

Malicious cyberoperations remain one of the most significant strategic threats to the United States, holding our national security, economic prosperity, the integrity of our democracy and public health and safety at risk. Over the past several years, network defenders in both Government and industry have seen the threat landscape grow more crowded, active, and dangerous. In fact, 2017 was one of the most costly and active in terms of global cybersecurity incidents, including the "WannaCry" ransomware incident attributed to North Korea and the "NotPetya" malware incident attributed to Russia. DHS and our interagency partners also worked with industry to identify and alert on Russian Government efforts to infiltrate domestic energy infrastructure.

But adversary actions did not begin or end in 2017. Russia's attempts to interfere in the 2016 U.S. Presidential election are well and widely known, as are their activities to interfere in other elections in Western Europe. With the 2018 midterm just around the corner, we are working aggressively to support State and local efforts to secure elections.

This partnership with election officials is representative of one of two core anchors of the U.S. deterrence strategy. Those two anchors are defense in depth to minimize or eliminate adversaries' success and impose costs with strong consequences from malicious behavior. My partner agencies here at the hearing have equities in both denial and consequences, but my organization, the National Protection and Programs Directorate, is almost exclusively focused on defense through protection of critical infrastructure.

Our approach is one of collective defense, emphasizing the shared responsibility of cybersecurity across industry and Government. We work through partnerships that identify stakeholder requirements, align unique capabilities to gaps, and add value and enable more effective security and risk management outcomes. We are focused on sharing information related to the threat and potential mitigation measures to improve defenses, leading integrated, coordinated industry and Government planning to address systemic risk, and conducting incident response to limit harm and inform defensive measures.

We manage these activities out of operational centers within NPPD, my organization, that prioritize collaboration across the full range of stakeholders—industry or Government. Our National Cybersecurity and Communications Integration Center, or NCCIC, operates at the intersection of private sector, State and local governments, Federal agencies, international partners, law enforcement intelligence, and defense communities. The operational focus of the NCCIC is near-term, day-to-day cybersecurity risk management, providing stakeholders with a 24-by-7 steady-state capability to address today's cybersecurity challenges.

We also work with stakeholders to develop information-sharing venues for affinity groups. Recently, working with election officials, we established the Election Infrastructure–Information Sharing and Analysis Center, or EI–ISAC. All 50 States participate in what is the fastest-growing ISAC.

The recently announced National Risk Management Center provides a forum for Government and industry collaboration on understanding risk and developing solutions for reducing cyber and other systemic risk to national and economic security. The operational focus of the National Risk Management Center is longer-term strategic risk, providing a cross-Government and industry capability to address tomorrow's challenges. Through the NRMC, we will partner with innovative industry coalitions like the Financial Systemic Analysis and Resilience Center and the Council to Secure the Digital Ecosystem, aiming to break down sector-based silos to craft a more holistic understanding of national risk and the integrated strategies to drive down that risk.

Our mission at DHS is to ensure that our stakeholders have the necessary tools and support to understand and act on risk. In the face of increasingly sophisticated threats, DHS is stepping up our

efforts to defend the Nation's critical infrastructure from malicious cyberactivity. We are working to better evolve our protection of critical functions from Nation-State and other malicious activities.

And before I close, I would like to thank Congress for the legislative progress thus far in strengthening DHS' cybersecurity and critical infrastructure authorities. Now we must move on to the next step: to create the Cybersecurity and Infrastructure Security Agency, or CISA, at DHS, which would see our organization, the National Protection and Programs Directorate, renamed and established as a new agency, an operational agency. Establishing this agency would enhance DHS' ongoing efforts as the focal point for private sector and Government stakeholders in support of our Nation's cybersecurity. We strongly support this much-needed effort and urge quick action by the Senate to pass this into law.

Thank you for the opportunity to appear before the Committee today.

Chairman CRAPO. Thank you.

Mr. Ford.

**STATEMENT OF CHRISTOPHER A. FORD, ASSISTANT SECRETARY, BUREAU OF INTERNATIONAL SECURITY AND NONPROLIFERATION, DEPARTMENT OF STATE**

Mr. FORD. Thank you, Chairman Crapo, Ranking Member Brown, and Senators. In light of the important role of this Committee in particular, as you outlined, Mr. Chairman, in international sanctions, I thought I would try to contribute today by explaining a bit of how we are employing the tools that Congress has given us vis-a-vis Russia in order to push back against the various malign activities of the Putin regime. I will focus in particular on Section 231 of CAATSA because that has fallen to my Bureau, the Bureau of International Security and Nonproliferation, to implement.

In passing CAATSA last year, Congress made very clear that its intention was to pressure Russia to change its behavior with respect to a very wide variety of malign acts, including in response to Putin's effort to interfere in our own Presidential election in 2016.

We have heard that message from Congress loud and clear, but I want to stress also that these sanctions tools have value in a broader arena of great-power competition and geopolitical competitive strategy. This is an important theme for our Administration.

The new National Security Strategy calls out "the contest for power" as "[a] central continuity in history," and it warns about challengers—specifically, "the revisionist powers of China and Russia, the rogue States of Iran and North Korea, and transnational threat organizations"—that are, as it describes, "actively competing against the United States and our allies and partners."

Similarly, Mr. Chairman, the National Defense Strategy observes that "[t]he central challenge to U.S. prosperity and security" today is "the reemergence of long-term, strategic competition." "It is increasingly clear," that Defense Strategy says, "that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other Nations' economic, diplomatic, and security decisions." The National Defense Strategy notes

that "[b]oth revisionist powers and rogue regimes are competing [with us] across all dimensions of power."

And this mindset, Mr. Chairman, is one that we bring to approaching CAATSA with respect to Russia. Russia has undertaken a campaign of malign activities in its attempt to compete with us, our allies and our partners. And CAATSA 231 gives us more tools with which to respond.

We are focusing in particular upon transactions with the Russian arms industry for multiple reasons. First of all, these are often the same arms that Russia itself uses and continues to use for aggression against Ukraine, for example. The world should shun transactions of that sort.

Second, as Willie Sutton is reported to have said when asked why he robbed banks, "That is where the money is." High-technology military equipment is one of the only competitive sectors of the Russian economy these days, and Moscow makes a good deal of money from selling arms abroad. These funds fuel the Kremlin's malign activities, spread its influence, and support Russia's development of newer and even more deadly weapons, and so we use sanctions tools to go after those revenues.

But, more broadly, Russia continues to use its arms transactions as a tool of geopolitical influence. For Russia, it is not just about money, but about the relationships that its arms trade creates. Scaling back and shutting down Russia's arms deals and deterring such transactions in the future strike directly at the Kremlin's malign activities and its influence, and that is the philosophy that we bring to implementing Section 231.

Naturally, we seek to cooperate with Russia wherever we can on issues of shared interest because that is important for the security of the world. But where we need to push back, we do so, and we do so hard. And we have hard real successes in using the availability of CAATSA sanctions and the threat of such penalties in deterring and dissuading transactions with the Russian arms business.

There are billions of dollars in transactions that have not occurred and will not occur thanks to the tools that Congress has given us and our ability to use those to provide diplomatic leverage. That is billions of dollars that Putin's war machine will not get and through which the Kremlin's malign influence will not spread, and a slew of relationships between the Kremlin and its would-be arms clients that will not occur or broaden or deepen.

So we have not yet had, in fact, the opportunity, the need to actually impose CAATSA sanctions yet, in part because we are in the business of trying to make sure that those dogs do not, in fact, bark. We want these things to be conspicuous by their absence, and we are making good progress in dissuading and deterring transactions from occurring.

We are not reluctant to do this, and if circumstances warrant, we will certainly be forthright and vigorous in applying the full breadth of the available penalties. But I want to stress how important our successes have been to date in making sure that billions of dollars of transactions do not occur.

In my written remarks, which I would ask, Mr. Chairman, be submitted as part of the record, I outline a series of principles

through which we approach implementation of Section 231. I would be delighted to talk about any or all of those as the course of the hearing progresses, but let me simply conclude by making the point that we are applying these as a vigorous tool of competitive strategy to make sure that we do as much as we can with those tools to undermine Russia's ability and willingness to use its malign behavior as a way to accrue its own strategic advantage around the world. We are starting to have significant successes here, and I would be happy to talk about these and take any other questions that the Committee would like as this time goes forward.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you, Mr. Ford.

I will start with you, Ms. Mandelker. As a number of you have said and we have said in our introductory remarks, there have been a number of sanctions imposed against Putin, his cronies, and the industrial apparatus they control. What type of sanctions have had the most impact on Putin? And what is the best strategy to change his behavior on either the Ukraine and cyberintrusions?

Ms. MANDELKER. Thank you, Chairman Crapo, for that question. We have had, as I already mentioned, well over 220 sanctions across the interagency since the beginning of this Administration, and the impacts of our sanctions have been felt in a number of very significant ways.

I would point as an example to the designations that we had in April against Russian oligarchs and very close associates to Putin, as well as a number of senior foreign officials. In addition to the oligarch sanctions, we also designated entities that were 50 percent owned or controlled by those that we designated, and as a result of those designations, we have seen a number of very significant impacts, as we have sent the clear message to those that surround themselves with Putin that there are very grave consequences for their involvement with him in malign activities around the world.

As you saw in those oligarch sanctions, the net worth of the individuals who we designated as well as the net worth of a number of other Russian oligarchs decreased substantially. The companies that they own or control similarly suffered great consequences. We continue to see the impact of those designations in a number of different ways.

Similarly, we have had very substantial designations against Russia's largest weapons trading company, against a very significant power company, energy company. Our sectoral sanctions not only remain in place since the beginning of the Administration, but thanks to CAATSA, we have tightened the directives that govern those sectoral sanctions. And, likewise, we are seeing a very significant impact on the Russian economy, on their energy projects, and the like.

Chairman CRAPO. Can Congress expect more designations from the Administration? And when?

Ms. MANDELKER. Absolutely, Senator. In fact, this morning we issued designations, Russia-related designations, both in connection with our North Korea program where we designated Russian shipping companies and business owners as well as Russian vessels. We also designated entities and individuals that have been involved in sanctions evasion by an entity that we recently des-

ignated in connection with their work with Russia's intelligence sector. Of course, we did so this morning, and you will without a doubt continue to see more from this Administration.

Chairman CRAPO. Thank you. Again, I do want to—I might have to come back and ask my questions of Mr. Krebs and Mr. Ford, but, Ms. Mandelker, Russian firms subject to sanctions have restrictions in place on their ability to borrow from U.S. capital markets. The Russian Government, however, can still sell bonds to U.S. investors and use the proceeds as loans to Russian firms under sanctions.

Does this ability to invest in Russian sovereign debt undercut the intent and effectiveness of existing U.S. sanctions?

Ms. MANDELKER. Senator, pursuant to CAATSA, the Treasury Department issued a report on Russian sovereign debt earlier this year. I know Secretary Mnuchin has commented on that report. I would leave it there. Of course, I know that there continues to be concern about ongoing investment with Russia which has as a general matter very significantly declined since the beginning of this Russia program.

Chairman CRAPO. All right. Thank you.

Mr. Krebs, the United States is currently in its primary and special election season right now. The 2018 midterm elections are now 11 weeks away, and you mention in your testimony that, as a result of assessing activity in the 2016 election, DHS is actively increasing awareness of potential vulnerabilities and providing capabilities to enhance U.S. and allied election infrastructure.

What authority or other help does DHS and its stakeholders need to better secure U.S. election infrastructure?

Mr. KREBS. Sir, thank you for the question. I certainly think that since 2016 we have made significant progress in terms of securing America's election infrastructure. As I mentioned in my opening statement, I think the one piece of legislation that I need within my organization is the Cybersecurity and Infrastructure Security Agency Act. I think that will streamline my organization and make us more effective in terms of engaging our stakeholders. You have to remember that my authorities are almost entirely voluntary, and so what I have to be able to do is clearly articulate who I am, what it is I do, and how I can help. And right now the National Protection and Programs Directorate does not really provide me that platform to describe those efforts.

Chairman CRAPO. All right. Thank you.

Senator Brown.

Senator BROWN. Ms. Mandelker, in April, our U.N. Ambassador announced that Russian companies who had helped Syria make and deploy chemical weapons would be sanctioned. On the Sunday shows she said that Secretary Mnuchin "will be announcing those Monday, if he has not already," and they will go directly to the sort of companies that were dealing with equipment related to Assad and chemical weapons use. The next day, those sanctions were pulled back, reportedly on orders from the President.

My question is this: When she spoke, had entities that aided in the chemical weapons attacks been identified and cleared through the usual interagency process?

Ms. MANDELKER. Senator, I am not going to get into interagency discussions. As you may be aware, in April we did designate

Rosoboronexport in connection with our Syria authorities. We have designated other Russian—and its subsidiary bank. We have designated other Russian entities in connection with our Syria——

Senator BROWN. I am sorry. I have a limited amount of time. Of course, the sanctions were pulled back that she announced, correct?

Ms. MANDELKER. Again, Senator, I am not going to get into——

Senator BROWN. Well, I know you do not—but the answer is yes or no, that the sanctions were pulled back?

Ms. MANDELKER. I am not going to get into those interagency discussions, Senator——

Senator BROWN. No, this is not an interagency discussion. This was—the sanctions were pulled back. I am not asking did President Trump do it personally. I am just asking, the sanctions were pulled back, correct, that she announced?

Ms. MANDELKER. We did not on that Monday announce additional Syria-related designations, but we have subsequently announced a number of very tough designations in connection with Russia.

Senator BROWN. I do not understand why you cannot tell me what happened. You do not want to go into interagency discussions, but you cannot tell me what happened. The sanctions were or were not pulled back. She announced them. They did not happen. That would suggest pulled back, stopped. Choose your own verb. You may not want to talk about what happened in the interagency discussions, but facts are facts, even today in this country.

Ms. MANDELKER. Again, you are asking me to comment on what happened within the interagency. Any particular set——

Senator BROWN. No, I am asking you—I am not asking you for discussions within the interagency. I am asking you, had the interagency actually identified and cleared them, and then what happened between her announcement and the inaction taken. But apparently you are not going to answer that.

Let me ask a question of you and start with Mr. Ford and then back to Ms. Mandelker. Powerful sanctions authorities Congress gave you last year, at least as applied so far, have not worked to compel Russia to scale back its aggressive behavior against the U.S. and its allies. All three of you spoke to that. There is still a lot of room for the Administration to use powerful authorities provided in CAATSA that this body 98–2 gave you on corrupt oligarchs and defense and intelligence sector most responsible for many of these cyberattacks, other areas.

If you would spell out, Mr. Ford, what is your plan to ratchet up pressure on the Kremlin in the short term prior to the elections to deter future attacks? Is it going after the personal assets of Putin and his cronies? Is it sanctioning State-owned entities like VEB, the Kremlin slush fund? Is it sanctioning Russia's sovereign wealth fund? What steps?

Mr. FORD. Thank you, Senator. With respect to influencing Russia's behavior, there are obviously several ways that we try to approach this. I mentioned the one of trying to cut back specifically their arms transactions influence and revenues.

More broadly, I would like to make the point also that this is only in part—obviously, the objective is to change Russia's behavior. But even were Russia's behavior not to improve as fast as we

wished that it would, we think that these approaches we are taking are having an impact in changing others' behavior toward Russia in ways that will leave Russia less able to engage in its ongoing campaign of malign activities. It will not have as many resources, as many partners with which to work. If we stigmatize dealings with Russia in varieties of ways, they will be less able to exercise that influence, even to the degree that they still wish to engage in it. That is part of the chilling effect that we seek to achieve by economic sanctions more broadly. It is part of the effect that we are trying to achieve across the board here as well.

So it is not just about influencing Russia directly. It is about having an influence upon the net impact of Russian behavior in the aggregate across the international community.

So with that as a predicate, I am not in a position to sort of forecast exactly what steps we will take. We are as a matter of very high diplomatic priority putting a lot of emphasis both with our partners, in conjunction with our partners, and directly to the Russians on the importance of them understanding that we are firmly of the view that this kind of malign activity and further activity of this sort to which you were referring, sir, were it to occur, we would continue to confront Russia with painful, sharp, and stern consequences. They need to know that.

Senator BROWN. Thank you, Mr. Ford. Is it especially important to announce bluntly and aggressively ahead of time what price Putin will pay if he engages in attacks on our elections?

Mr. FORD. We are making it very clear, Senator, that there will, of course, be consequences, and painful ones, if they engage in additional unacceptable conduct. We also think it is important not to be too specific about that. This is not a game of forecasting or trying to encourage the Kremlin to study to test. But it is a game in which we are making it very clear that this behavior is not acceptable and will not be tolerated. We are trying to do that mindful of all of the things with which we agree with Congress.

It has been very clear, for example, in talking about CAATSA legislation that there is a powerful desire here in Congress, which we share, to signal that Russia's malign activities are unacceptable and to try to deter them in the future.

We also understand and agree with what appears to be Congress' clear view that it is important to do that in ways that do not have grave and unforeseen consequences for other aspects of our U.S. interests, whether that is issues of U.S. jobs and the economy and competitiveness or the relationships that we need to maintain with allies and partners and friends around the world, including that are important to us with respect to Russia policy.

So we are trying to find the sweet spot between all of these various competing approaches, and we are grateful for the tools that Congress has given us to provide diplomatic leverage to that effect.

Chairman CRAPO. Senator Kennedy.

Senator KENNEDY. Thank you, Mr. Chairman, and I want to thank my colleagues for letting me jump the line here.

Ms. Mandelker—am I pronouncing your name right?

Ms. MANDELKER. Yes, Senator.

Senator KENNEDY. OK. Does Mr. Putin personally own assets in the United States?

Ms. MANDELKER. Senator, I would defer to my colleagues in the intelligence community, and I would be happy to talk to them about providing you a briefing on that subject.

Senator KENNEDY. Well, they are not here, but you are. So let me ask you again. Does Mr. Putin personally own assets in the United States?

Ms. MANDELKER. Again, Senator, that is not something that we can discuss in an open or public setting, but we would be happy to sit down with you and provide a classified briefing with our intelligence community colleagues.

Senator KENNEDY. Mr. Krebs, do you have anything to add to that?

Mr. KREBS. No, sir.

Senator KENNEDY. How about you, Dr. Ford?

Mr. FORD. No, Senator.

Senator KENNEDY. OK. If he did personally own assets in the United States, why would we not as a sanction consider seizing them, hypothetically?

Ms. MANDELKER. Hypothetically, Senator, if any Russian oligarch or senior leader had assets in the United States, of course, that is an action that we would consider undertaking, assuming it is within our legal authorities to do so.

Senator KENNEDY. Well, this is just my opinion, but here is what I think: I think Mr. Putin does own assets in the United States, and I think that Treasury knows what those assets are. And whether we do it in a classified or unclassified setting, that is above my pay grade. But I would like us to have a frank and honest discussion about the ramifications of seizing those assets. Would you object to that?

Ms. MANDELKER. Not at all, Senator.

Senator KENNEDY. OK. Last question. Dr. Ford, let us suppose that the President of the United States came to you and said, "Look, I have had enough. Crimea, Ukraine, Syria, chemical weapons, meddling in American elections. I hate to do it, but I want to bring the Russian economy to its knees." How would you do that?

Mr. FORD. Well, Senator, I am afraid I am not enough of an economist to have a real crisp, off-the-cuff answer for you. I certainly would hope and expect that we would approach any challenge the President gives us with the kind of——

Senator KENNEDY. Excuse me for interrupting. I want to keep my—it sounds like you are not going to answer, so no offense, I am going to keep moving.

Mr. Krebs.

Mr. KREBS. I would have to defer to the other experts. We are focused on defending American infrastructure.

Senator KENNEDY. All right. That is fair. I appreciate your candor.

Ms. Mandelker.

Ms. MANDELKER. Senator, were we to have any conversation along those lines, of course, we would want to consider what the global ramifications would be of taking those kinds of actions. So as I have already mentioned——

Senator KENNEDY. OK. Let us put the global ramifications to the side for a moment, though; then we can talk about the ramifica-

tions. Your task is to bring the economy to its knees. How would you do that?

Ms. MANDELKER. Again, Senator, I do not think you can have a discussion about how to bring Russia's economy to its knees without having a full understanding of what the global consequences would be of taking certain kinds of actions. We have——

Senator KENNEDY. OK. Well, how about telling me what you would do and then telling me the consequences so we do not get the two mixed up?

Ms. MANDELKER. Again, Senator, we have taken a number of very aggressive actions targeting the Russian economy——

Senator KENNEDY. I know that.

Ms. MANDELKER. ——in very strategic, targeted, and impactful ways.

Senator KENNEDY. But the economy has not been brought to its knees. Look, I do not want to use my time—if you are not going to answer the question, just tell me.

Ms. MANDELKER. Again, Senator, we would be happy to have a conversation with you about that, but I think it is important that in any conversation where we are talking about very significant actions, we also have an understanding of what the global consequences would be. I think that is the responsible way to have that conversation.

Senator KENNEDY. I just asked you to tell me those. I am out of time. Sorry, Mr. Chairman. Sorry, guys, I could not do any better. I tried to get answers.

Chairman CRAPO. Senator Menendez.

Senator MENENDEZ. Thank you, Mr. Chairman.

I just came back from the Senate Foreign Relations Committee, which is also having a hearing on U.S.–Russia policy, and while that Committee obviously deals with foreign policy, this Committee's jurisdiction over economic tools to promote our foreign policy is incredibly important, so I appreciate today's hearing.

Let me just ask you all, clearly, notwithstanding what the Congress has passed into law, what the Administration has enforced through your own testimony elements of that law, it is fair to say, is it not, that Russia has not been deterred in its actions and malign activities? Is that a fair statement?

Ms. MANDELKER. I think, Senator, we are seeing a number of consequences as a result—and impacts as a result of the actions that we have taken. There is no question that we continue to see Russian malign activity and Russian malign——

Senator MENENDEZ. Well, today Microsoft announced that, in fact, there are attacks on the U.S. Senate and on some venerable conservative institutions. That is a continuing action. As far as I know, Russia is still annexing Crimea and engaged with their regular forces in Eastern Ukraine. As far as I know, Russia is propping up Assad in Syria. And I could go down through a list.

So for the most part, I think it would be fair to say that Russia has not been deterred in terms of its activities.

Ms. MANDELKER. I think it is very fair to say that Russia is continuing to engage in a wide range of malign activity that causes us grave concern.

Senator MENENDEZ. OK. So on that we are agreed.

Now, with that as something that is a reality, obviously what we are doing, notwithstanding all the efforts of Congress and the Administration to date, has not deterred them in these malign activities in a way we would like to see, which is the purpose of sanctions in the first place.

So I know that Senator Graham and I have legislation called "Defending American Security From Kremlin Aggression." I know that my colleague on the Committee with Senator Rubio also has the DETER Act. I am sure there are other initiatives. Maybe the Chairman is thinking of some with Senator Corker.

The bottom line is instead of telling us what is wrong with these ideas and pieces of legislation, why don't you tell us what, in fact, we can do to turn up the pressure on Moscow that we are not?

Ms. MANDELKER. Senator, you know, in the last year, as you have seen, we have taken a number of very aggressive actions in connection with our Russia sanctions program, including a number of actions under——

Senator MENENDEZ. Madam Secretary, I do not need you to regurgitate and eat up my time by telling me what you have done. What you have done we have just collectively agreed has not moved the ball in a way we would like to see. So what I am saying—it is not a confrontational question. It is a question of—Congress is going to act. You might as well know that. I have been through Administrations, both Democratic and Republican, who did not want to see sanctions legislation. At the end of the day, Congress acted and many of them subsequently learned that what we did was the best tools that they had to try to move foreign policy. So it is going to act. I would rather it act in a way that has your insights about what would be helpful, but if you fail to provide insights, then we will provide you with a law that ultimately will take place without your insights. So that is all I am seeking here.

If you are telling me—and this question is collective—there is nothing more that we can do than what we are doing, if that is the answer, that means that Russia will continue to do all the things I said before, nothing more that we can do than what we are doing is going to change the course—and that is a sad state of events for not only our country but the world. Is that what you are telling me?

Ms. MANDELKER. Senator, we would be happy to work with you on any particular piece of legislation. What I can tell you is that we have a broad range of authorities currently in place that we have been very actively using——

Senator MENENDEZ. OK, with all due respect, I have heard you say this. You are very good at repeating the same thing, but it does not help me.

So let me ask you this: The expectation among Senators is that you will continue to impose sanctions on oligarchs, but it seems to some of us that you have decided to diminish pressure. You have not designated any oligarchs since April 6th. You have delisted Estonian banks, and now there are reports that you may delist Rusal.

What kind of signal does that send to the Kremlin? We are told to judge the Administration by its actions and not the President's words, but these actions seem to be more in line with the President's accommodating and disturbing rhetoric than a tougher ap-

proach to the Kremlin. So why haven't you listed any oligarchs since April 6th? And why are you delisting these other entities?

Ms. MANDELKER. Senator, we have designated a number of additional Russian-related entities since April 6th. It is a very active program for us, including a number——

Senator MENENDEZ. I mentioned specifically oligarchs, not entities.

Ms. MANDELKER. A number this morning. I am not going to preview what our plans are, but we continue to look very carefully at the oligarch report, and it continues to inform our actions.

Senator MENENDEZ. Secretary Ford, let me—so the answer is you have not listed anybody else and you are delisting people.

Let me ask you this, Secretary Ford. I understand your office implements Section 231. Convince me that your leverage to convince individuals to not purchase Russian defense equipment has somehow been strengthened by the new waiver provisions included in the National Defense Authorization Act. You have not imposed one sanction under this provision, not the new provision with waivers. You have not imposed one sanction under Section 231. Why?

Mr. FORD. Well, Senator, what we have been stressing to our diplomatic interlocutors is that, unless and until something—well, of course, under the statute there has to be a significant transaction. We stress to our interlocutors that——

Senator MENENDEZ. Clearly there have been those.

Mr. FORD. Well, no determination of significance has been made yet, sir. It is important to stress that our focus has been, as I indicated earlier, upon making sure as best we can that transactions do not occur. Obviously, if they do, we will, of course, evaluate its significance and reach a determination as quickly as the bureaucratic process permits. It is important to how we are approaching this to make sure that our interlocutors understand that what we are trying to do is, in fact, implement our own priorities and Congress' priorities upon doing two things simultaneously.

One, of course, we need—and it is imperative to do so, we need to make sure that Russia feels pressure from this. The objective is to change Russia's behavior and, therefore, pain needs to be felt. And the point is to bring that pain. But the pain is against Russia, not against our friends and allies. And we also understand Congress was very clear in passing CAATSA also that this needs to be done in a way that is mindful of the importance of protecting the relationships that we have and that we need in our diplomacy and our foreign relations and our national security affairs around the world with people who may have had engagement with the Russian arms business but whom we do not want to simply throw away our relationship with. So we are trying to do those two things at the same time, sir.

Chairman CRAPO. Senator Scott.

Senator SCOTT. Thank you, Mr. Chairman. Thank you to the panel for being here this morning.

I certainly want to echo the comments of the Ranking Member, the Chairman, and many of the Senators that reflect the importance of finding ways to constrain Russian aggression, especially as it relates to our country. And it seems like to many of us that our efforts have just not been effective enough.

If you look at from 2014 and forward, the sanctions, we have sanctioned hundreds of Russian entities in response to the annexation of Crimea, their human rights abuses, their cyberattacks, their support of the Assad regime, weapons proliferation. The list continues to go on and on and on to the Russian aggression, and yet there is so little that we can show for our efforts of sanctioning Russia.

I have two questions. One is about understanding the certain sections of CAATSA that have yet to be implemented and what steps we can take to ensure that our policies are able to achieve the desired outcome. That is the first question.

The second question is: While we are looking at the implementation of more sections of CAATSA, how do we protect our American businesses as it relates to the negative impact that will come from it?

So I understand that you all are in an incredibly sensitive position trying to do two things that are actually not mutually exclusive but really weigh heavily on one another. The challenge of Senator Kennedy's question that it is really a simple answer, frankly, if 70 percent of Russia's exports are in the energy sector, it seems to me that the clear, simple answer is that if you wanted to have the most impact that has the ability to cripple the economy, the answer is in the energy sector. Perhaps the challenge is that the energy sector represents the sector that many of our allies in Europe depend heavily on. So it does make your task challenging, but the fact of the matter is that there is a very simple, clear, concise answer to Senator Kennedy's question, which is that if 70 percent of the Russian economy—perhaps not 70, maybe it is 68 percent—flows through the energy sector, the answer is simple. I am not quite sure why we are having such a difficult time answering simple questions. We seem to be more evasive than helpful in our desire to understand and appreciate the magnitude of our actions on the Russian economy. And when there are sections beyond Section 224 that deal specifically with crude oil exports, or Section 226 and 227 and 228, and Bob mentioned 231 and 232 and 233 and 234, the answers are all the same, that we have not done much in those sections.

I would come back to my original question; that is, as we look at CAATSA, how can we do more? It seems like I have just given you a list of options on doing more. And why aren't we? And is the answer to my second question that the impact on our businesses is creating headwinds on our ability to impose more sanctions and do more damage to the Russian economy because we are afraid of what it does to our businesses and to our allies?

Ms. MANDELKER. Thank you for your question, Senator. So just with respect to the very specific provisions of CAATSA, as you may be aware, we have designated over 160 entities and individuals under authorities that are either subject to a specific provision of CAATSA or Executive orders that have been codified by CAATSA. So our desire to implement and our execution of the implementation of CAATSA is very strong.

Very specifically in the energy sector, not only have we designated entities under our energy authorities, but Russia's energy sector is subject to two directives—Directive 2 and 4—that were

started in the Obama administration and which we have tightened in this Administration. And we have seen significant impact as a result of those designations.

You asked about U.S. businesses. Well, Exxon announced earlier this year that they were withdrawing from joint venture projects in Russia with Rosneft. Similarly, we heard—it was announced that Rosneft was unable to complete certain projects in the Black Sea. Because of our sanctions, they were unable to get the kind of equipment and technology that they need in order to do so.

Senator SCOTT. Thank you. Because I have 25 seconds left and the Chairman already called one Member down for going over time, I do not want to be the second Member, so I will not go over the time by that much. But I will just say that perhaps you would invest all of our time more wisely if we talked about the interconnectedness of the global economy and how at times if Russia is working with Saudi Arabia on output in order for us to have a more positive impact on Iran through our, you know, withdrawing from the JCPOA, we would have a more global and panoramic perspective on the challenges and consequences and the complexities of the task at hand, and we would have a more productive time in understanding and appreciating the challenges that you face, and at the same time be able to talk to our constituents about the challenges that we face, especially as the *Wall Street Journal* today reported that Russian hackers target conservative groups and widening cyberattacks, which only suggests that whatever we are doing is not enough.

Thank you, Mr. Chairman.

Chairman CRAPO. Senator Tester.

Senator TESTER. Thank you, Mr. Chairman.

I want to thank you all for being here, and I appreciate your testimony, although it would be nice to get answers to the questions. I am as frustrated as the folks who come before me.

So let me ask you this, Ms. Mandelker, and it is an honest question because I do not know the answer to it. Say I have got a $10 million ranch and I sell it to somebody who wants to launder money for $20 million, and they turn around and sell it for $15 million. Is that money then laundered?

Ms. MANDELKER. It would depend on the facts and circumstances, but that sounds like a situation where money was laundered.

Senator TESTER. OK. And is that legal?

Ms. MANDELKER. If it is here in the United States, that could potentially be a violation of our money-laundering laws.

Senator TESTER. OK. And is that something that we do, we go after folks who are trying to launder money? Is that something the Treasury Department does?

Ms. MANDELKER. Absolutely, Senator.

Senator TESTER. It does?

Ms. MANDELKER. Well, again, the criminal authorities are the Justice Department's authorities, but we go after illicit activity, money laundering, all over the world in a variety of different ways.

Senator TESTER. Can you tell me or can you get back to me on how many money-laundering episodes in the last 5 years have occurred and how many have been actually prosecuted?

Ms. MANDELKER. Again, in terms of prosecutions, I would defer to the Justice Department——

Senator TESTER. Determined and turned over to the Department of Justice. How about that way?

Ms. MANDELKER. I am sorry?

Senator TESTER. Determined that it was a money-laundering situation and turned over to the Department of Justice. We will deal with their prosecution later.

Ms. MANDELKER. Again——

Senator TESTER. Can you give me an example of how many have happened in the last 5 years? How many have been brought forth in the last 5 years by the Department of Treasury, not prosecuted but just pointed out by the Department of Treasury that they had grounds?

Ms. MANDELKER. I cannot give you a number. We work——

Senator TESTER. Can you give me a number if you go back to your office and write it down on a sheet of paper and send it to my office?

Ms. MANDELKER. Again, Senator, it would depend on the specifics of your——

Senator TESTER. Is this—no, no, no, no, no.

Ms. MANDELKER. ——question, but we work very closely with the Justice——

Senator TESTER. Look, look, we had one of these hearings in a classified session that was worthless. And it was not worthless because of the Chairman and Ranking Member. It was worthless because you guys have filibuster down to an art. I just want to know the answer to the question. Do you have the number, yes or no?

Ms. MANDELKER. Is your——

Senator TESTER. You do not have the number?

Ms. MANDELKER. I want to make sure that I understand the question you are asking.

Senator TESTER. I want to know the number of money-laundering episodes the Department of Treasury has turned over to the Department of Justice in the last 5 years—not 10, not 20, not 30. Five years, that is it.

Ms. MANDELKER. Again, Senator, as you may be aware, FinCEN——

Senator TESTER. I am not aware. I just want to know how many.

Ms. MANDELKER. I would have to go back to my office to see——

Senator TESTER. OK. Go back to your office and you will——

Ms. MANDELKER. ——if we have such a number.

Senator TESTER. ——give me that information?

Ms. MANDELKER. But I just want to be clear about what it is that we do. We follow, we trace, we track money laundering all over the world. We are also the recipients——

Senator TESTER. I just want to know about the stuff that happens in the United States. That is easier yet.

Ms. MANDELKER. Let me go back and see what we can do to answer your question.

Senator TESTER. I appreciate that very, very much.

Mr. Krebs, you said in an answer to the Chairman's question that you have made significant progress since the 2016 election.

Can you give me a list of the things you have done to make our election more secure this cycle?

Mr. KREBS. Yes, sir. So four buckets: governance, information sharing, technical support, and incident response.

Senator TESTER. OK. And have you done that to every State in the Union?

Mr. KREBS. We work particularly through the Election Infrastructure ISAC. We work with all 50 States. We provide cyber remote-scanning capabilities to 36 States.

Senator TESTER. I do not expect you to know this today, but can you go back to your office and send me a list of what you have done in Montana specifically?

Mr. KREBS. We can certainly give you a briefing on the things we are doing nationwide.

Senator TESTER. Just give me a sheet of paper. I do not need a briefing. Tell me the things you have done in Montana to help Montana have a more secure election cycle.

Mr. KREBS. We can follow up, yes, sir.

Senator TESTER. And just a suggestion. It might not hurt to do that for every Senator that is here. It would be a good thing. Just what—I see Donnelly is nodding his head, so you can do that for Indiana, and——

Mr. KREBS. We do need to—there is a certain degree of confidentiality on every engagement——

Senator TESTER. Oh, come on. These guys—now, look, look, look. If these guys are screwing with voter rolls, tell us how you fixed it. If they are screwing with voter machines, tell us how you fixed it. There is no security there. This is about confidence in our election system. Putin spent less money on doing what he did last cycle to promote communism and destroy democracy. I think the U.S. Senate needs to know this stuff.

Mr. KREBS. I agree, yes, sir. Let me——

Senator TESTER. Just give us the information.

Mr. KREBS. We can follow up. Yes, sir.

Senator TESTER. OK. Thank you.

Then can anybody tell me why Putin's ownership of anything in this country is not public information?

Ms. MANDELKER. Again, Senator, as I mentioned before, we would be happy to sit down and have a conversation with you about that.

Senator TESTER. I do not want—just tell me. Why? What national security risk is that?

Ms. MANDELKER. Again, Senator, any discussion about where assets are in the United States or elsewhere are either classified or not something that we would discuss in any kind of an open session.

Senator TESTER. You do know that you can go down to the courthouse and find out how much land I own? You know that. So why is Putin different?

Ms. MANDELKER. Again, Senator, I do not want to talk publicly about where assets are here or anywhere in the world. There are a number of different reasons——

Senator TESTER. OK. I got that.

Ms. MANDELKER. ——why we would not do that, but having had——

Senator TESTER. But a yes or no does not exactly——

Ms. MANDELKER. ——a sitdown and having a conversation——

Senator TESTER. A yes or no does not dictate section, township, and range. A yes or no just says, yeah, he owns property here.

Ms. MANDELKER. Senator, I am not aware of any title or deed that would have Mr. Putin's name on it here in the United States. But, again——

Senator TESTER. All right. All right. Thank you very much. OK. Thank you, Mr. Chairman.

Chairman CRAPO. Senator Cotton.

Senator COTTON. Thank you, Mr. Chairman. Thank you all for appearing here. I hope it is clear from the questions so far that we have bipartisan agreement about the threat that Russia poses to our democracy and our interests. It is good to have that agreement now, which we lacked for many years. In the last Administration, even as Russia was surging troops into Syria to prop up Bashir al-Assad and Iran and invading Crimea and waging war in the Ukraine and beating a United States diplomat on the doorstep of our embassy in Russia and flagrantly violating the Open Skies Treaty and flagrantly violating the Intermediate Range Nuclear Forces Treaty and a whole host of other malign activities.

Now, we have heard a lot today that Russia is still not deterred from these things. I would agree with that. We need to take additional action. But we have not heard much about the relative impact of the steps that this Administration has taken versus the last Administration, in particular after the 2016 election.

Now, some members of the last Administration said that they did not want to take provocative steps in the fall of 2016 because they feared that Vladimir Putin and Russia's intelligence services might take additional steps to undermine voter registration systems or vote tabulation systems. But after the election, the Administration kicked out a few Russian diplomats—it might not surprise you to know that those were perhaps Russian spies—closed two Russian vacation homes, and imposed sanctions on two Russian intelligence services.

Ms. Mandelker, how much money did the U.S. Government get from those two intelligence services?

Ms. MANDELKER. Senator, I am not aware of assets that were blocked as a result of those——

Senator COTTON. Is that perhaps because Russian intelligence services do not keep money in the United States banking system?

Ms. MANDELKER. Again, Senator, that is not something I would discuss publicly, but rest assured the designations that we have had in this Administration have had far and wide-ranging impacts in a variety of different way.

Senator COTTON. To say nothing of nonsanctions activities, for instance, like encouraging our NATO partners to spend more money on their defense, expanding our nuclear arsenal, spending more money on ballistic missile defenses, providing the antitank Javelin missiles that Ukraine's Government begged for so long to receive.

The Congress has also learned over the last 18 months that there was a serious interagency conversation in November and December

of 2016 about imposing tougher sanctions on Russia. In fact, I understand that the professional staff at the Treasury Department worked up a whole host of sectoral sanctions and specific sanctions against Russian companies like Kaspersky Labs. Yet those were strongly opposed by Secretary Jack Lew, National Security Adviser Susan Rice, and Deputy National Security Adviser Avril Haines.

Ms. Mandelker, can you explain why Secretary Lew opposed taking tougher action after the election—after the election, not before the election. After the election.

Ms. MANDELKER. Senator, I was not in the Administration, of course——

Senator COTTON. Though you are a representative of a the Treasury Department, which surely has continuity files.

Ms. MANDELKER. What I can tell you, Senator, is that, as I have already made clear today, we have gone after very significant and impactful designations in connection with Russia's election interference, in connection with their cyberattacks, in connection with their ongoing occupation of Crimea and the like, and we have seen those designations result in very impactful actions against, again, some of Putin's closest allies and partners, his senior foreign official, officials in his Administration. We have seen companies who have tried to get into Crimea have a very heavy cost imposed upon them when we have sanctioned them. They have cutoff their ability to do business elsewhere in the world.

What I can do is speak to the very heavy costs and impact of the designations that we have had. They have been quite substantial, and I would say far more substantial than those that were issued immediately after the November 2016——

Senator COTTON. It would be nice to know why Secretary Lew believed that and why President Obama accepted his opinion.

Let us take one final question here about a gentleman you mentioned earlier: Oleg Deripaska, a Russian oligarch whom our Government has sanctioned. You have also sanctioned numerous companies that he runs or heads, such as Rusal, En+, Basic Element, and others.

We now know, in fact, we have emails right here that have been released by the Congress between Christopher Steele, who compiled what Jim Comey called "a salacious and unverified dossier," and Bruce Ohr, a senior Department of Justice official in the Obama administration, where Christopher Steele was advocating on behalf of Oleg Deripaska being admitted into the United States. Christopher Wray, the FBI Director, would not address a question I sent to him in a public hearing of the Intelligence Committee earlier this year about whether Christopher Steele was working for Oleg Deripaska. At the time, by all appearances, he is working for him. Is Christopher Steele and his business the kind of entity or subcontractor for a sanctioned Russian oligarch that you have the authority to sanction under CAATSA?

Ms. MANDELKER. Senator, I am not going to talk to any particular individual, but Oleg Deripaska has been designated, and that designation is subject to secondary sanctions. And so what we have seen as a result of the Deripaska and other sanctions against these oligarchs is that they have become radioactive as the world

understands that any entities that they touch may similarly face severe consequences.

Senator COTTON. Just one final question. Just yes or no. It is a question about a general legal principle. Do you have the authority under CAATSA or any other law to sanction professional service providers of sanctioned Russian oligarchs, lawyers, lobbyists, financial advisers, and so forth?

Ms. MANDELKER. We would likely have that authority, Senator.

Senator COTTON. Thank you.

Chairman CRAPO. Senator Warner.

Senator WARNER. Thank you, Mr. Chairman. I appreciate the witnesses' testimony.

I think the indication from Microsoft today of ongoing Russian targeting of our elections and our systems is showing that this is not something that is in the rearview mirror. The truth is manipulating social media is both cheap and effective, and Putin and his cronies realize that. I think it reinforces, and if there is one message that ought to be taken out of this hearing, it is that we all need to stay focused. And that focus ought to extend—and I have some sympathy for you, Mr. Krebs, in terms of trying to make sure our State and local election partners take this message seriously and recognize that this is not all in the rearview mirror, that none of these activities stopped in 2016. They are ongoing, and this is an ongoing threat. And I am particularly concerned about that last-mile issue of even if we notify, will they then take action?

Ms. Mandelker, as I indicated to you beforehand and one of the things our Intel Committee investigation is looking back into in terms of Russian activity, we need your assistance. So I need your public commitment today that those outstanding document requests we have to FinCEN will be met in a timely manner.

Ms. MANDELKER. Senator, as you know, we have produced thousands of documents——

Senator WARNER. But not all of the documents have been submitted. Will you meet our bipartisan requests for those documents?

Ms. MANDELKER. Absolutely.

Senator WARNER. There has also been a BuzzFeed story that says that FinCEN has decided that some of those documents will not be turned over to the Committee. Will you refute that story and say that all documents that the Committee has requested will be turned over to the Committee?

Ms. MANDELKER. I am not aware of that story, but I can assure you that we are going to continue to produce documents that——

Senator WARNER. All documents in a timely manner, within the next 30 days? Within the next 60 days?

Ms. MANDELKER. I would have to consult with those who are reviewing the——

Senator WARNER. Many of these documents have been requested literally for months.

Ms. MANDELKER. But we commit to you that we will continue to produce those documents on top of the thousands of——

Senator WARNER. In a timely process so that we cannot——

Ms. MANDELKER. Absolutely.

Senator WARNER. Again, we are 7, 8 months behind on some of these document requests.

Ms. MANDELKER. We will absolutely continue to provide those documents.

Senator WARNER. And then one of the things—we have made a formal request to you in the past, but I want to reiterate in a public forum, because of the nature of some of these documents that are fairly complicated, we need your office's technical assistance in terms of interpretation of these documents. Will you be able to provide that technical assistance?

Ms. MANDELKER. Senator, let me just add to my last response. I am told that we have a document production that we will be providing today, and as I mentioned before the hearing, we are happy to provide additional assistance.

Senator WARNER. But what we need is that technical assistance to sort through this. I appreciate that.

Mr. Krebs, again, I mentioned—and you indicated you have got only voluntary ability to work with those on the front line. One of the things I have grave concerns about. In a normal White House, when our country has been attacked, as it has been, in this bipartisan consensus, there would be someone designated in the White House as election security is a top matter or someone designated on the National Security Council as making this a top priority.

One of the things that has been extraordinarily disturbing to me is we have had repeatedly top intelligence officials from the Trump administration indicate to us that they have not been told that election security ought to be a top priority, and that raises huge concerns to me, recognizing that you are trying to do your best at DHS. One of the questions—I have got a serious of questions for you here, recognizing I have only got a short amount of time. Is there any intention—we have sanctioned the IRA officers indicated by the Mueller indictments. Is there any effort to indicate or to sanction the 12 GRU officers that were also designated in the Mueller indictments?

Ms. MANDELKER. Senator, as you are aware, we have sanctioned a number of individuals connected to the GRU and the FSB. In fact, some of the sanctions we issued this morning were specifically in connection to their relationship to the FSB. We did designate the——

Senator WARNER. The IRA but not some of the 12 GRU——

Ms. MANDELKER. We are very closely looking at that indictment. I cannot preview what our plans are, but rest assured that——

Senator WARNER. All I will say is it would help, I think, the American public, as we sanctioned these bad actors and these bad actors' identities and a case that was built against them was provided by the actions and workings of the special prosecutor. It would do a great deal of benefit to the American public in terms of the seriousness of this threat if the President of the United States would not on a daily basis denigrate the Mueller investigation and call it a "witch hunt," an investigation that has created 30-plus indictments, a number of guilty pleas, and obviously has been a very valuable tool in identifying these bad actors who in the past and on an ongoing basis try to interfere in our election activities.

Mr. Krebs, do you have indication of who attacked Senator McCaskill's activities, a Senator up for reelection, other elected offi-

cials? And what level of confidence do you have in terms of overall Russian activities toward current sitting elected officials and/or elections that are coming up in a few months?

Mr. KREBS. So to the second question, certainly, I think, Congress is a target for foreign intelligence collection just based on your role in policy formation. So there are general espionage and foreign intelligence collection concerns there, with or without a midterm or a Presidential election coming up across the horizon.

Now, the Microsoft, whether it was McCaskill or the recent announcements, they have been in contact, as I understand it, with DOJ and FBI. We have also had conversations with Microsoft to get a better understanding of what they saw that enabled them to take action. In terms of a formal attribution from the Government, I would have to defer to the intelligence community on that.

But, again, rest assured we are engaging on a day-to-day basis with the Senate CIO, the House CIO, with the committees, and I would encourage you to encourage your staff to work with the Department of Homeland Security. And more than that, when you do go back to your districts or when you go back to your home States, please encourage your State and local officials to work with the Department of Homeland Security on election security matters.

Senator WARNER. I think it is important then to make sure that, as you contact States, you indicate that this is an ongoing threat. It did not end in 2016. And, unfortunately, some of your communications to States within the last week or so have not had that kind of clarity.

Mr. KREBS. I am happy to follow up, and I look forward to tomorrow's closed session.

Senator BROWN. Mr. Chairman, if I could, I just wanted to reinforce, in Senator Warner's admonition and request, how the important these documents are that they be turned over in a timely manner. Thank you.

Ms. MANDELKER. We appreciate that, Senator, and as I mentioned, we are dropping off another production today. We have a big staff who have been working to get these requests out quickly.

Chairman CRAPO. Senator Moran.

Senator MORAN. Chairman, thank you very much.

I direct this first question to any and all. Can you identify changes in Russian behavior that have occurred since the summit between President Trump and President Putin in Helsinki? Different behavior by Russia than before the summit?

Mr. KREBS. I do not have anything to add. No, sir.

Senator MORAN. Anyone?

Ms. MANDELKER. Senator, I would ask that any kind of question like that be addressed in a closed session.

Senator MORAN. We have had a closed session, and I share the view of the Senator from Montana that getting answers in a closed session is no easier than getting answers in an open session.

Ms. Mandelker, your unwillingness to answer the question—one of the things I thought would come from this hearing is a recommendation or a set of recommendations of what Congress might consider legislatively for additional sanctions. I have not reached any conclusion that additional sanctions are beneficial. I do not know the answer to that question. But I would have thought that

you could have been able to give us ideas of what we might look at or pursue in cooperation with you and the Administration.

Am I to take from your unwillingness to answer that kind of question that there is opposition by the Administration to additional sanctions? Or what is a better explanation?

Ms. MANDELKER. Senator, absolutely not. There is no opposition to sanctions. As I have already mentioned, we have designated well over 200 individuals and companies in connection with Russia——

Senator MORAN. I am talking about additional sanctions, something that we are looking at in this Committee.

Ms. MANDELKER. Including additional sanctions that we issued just this morning. In terms of what additional authorities we may need, we already have, through CAATSA and through a variety of different Executive order, brought authority to target big sectors of the Russian economy, to go after the Russian oligarchs, to go after Russia's malicious cyberactivities in a number of other areas. In fact, as I have already mentioned, we have targeted not only a number of very significant Russian companies, we have targeted the chairs of those companies, making it much more difficult for them to operate in the world.

So we would be happy to sit down and talk to Congress about any proposed legislation, but we do have significant and substantial authorities already on the books.

Senator MORAN. And maybe that is the answer to the question. It is not what you have been able to do, but the answer to the question what more do you need is nothing is known at the moment but you will consult with Congress if we come up with an idea, is my takeaway from your testimony.

I think I generally agree with Senator Cotton that we ought to be looking at other issues in addition certainly to sanctions, which is our relationship with NATO, economic alliances around the globe, resolving our trade differences with other countries so that we are unified. I think the list is longer than sanctions. We generally are focused on sanctions in this Committee, but I take it from your answer that to date you believe you have the necessary authorities to combat what we are trying to combat with Russian behavior. Is that a fair assessment?

Ms. MANDELKER. Yes, Senator, but we are happy to talk to you about——

Senator MORAN. Happy to have that conversation.

Ms. MANDELKER. ——additional authorities, and I agree with you wholeheartedly, this is a whole-of-Government approach. Sanctions alone are not going to solve the problem, and this Administration has undertaken a number of additional activities in connection with the Russian threat other than sanctions.

Senator MORAN. Thank you very much.

The Administration—I think is probably—I do not know who this is for. The Administration has called for a complete cutoff of Iranian petroleum imports by November. That seems to me to be just in time for winter. Does it stand to reason that that will push Europe and others to be more dependent upon Russian oil and natural gas? And is there coordination on the sanctions that we are proposing pursuing with Iran and sanctions that we have in place with Russia or are proposing with Russia?

Ms. MANDELKER. Absolutely, Senator, there is extensive interagency coordination on those sanctions with the State Department, with the Department of Energy, and, of course, with our closest allies and partners.

Senator MORAN. Mr. Krebs, in your testimony you note the leadership role that the Department plays in conducting elections, coordinating efforts to assess vulnerabilities and mitigate risk. Within this structure, DHS also plays an important role in sharing information with election officials. I have visited with county clerks, county election officers in Kansas, with personnel within our Secretary of State's office that conducts oversight and management of elections in our State.

What steps has DHS taken to ensure that information and intelligence is shared with local officials? My general impression is that while there is concern by election officials, they do not know the direct nature of any threat.

Mr. KREBS. So we have prioritized security clearances for State and local election officials. I think right now we are up to about 92, and that includes every single State. But most importantly——

Senator MORAN. Is an election official somebody at the State level or somebody at the local level?

Mr. KREBS. It started, yes, sir, at the Secretary of State or the chief election official in each State, and we are working our way down to the county level. Now, I do not think we are going to get to the county level in terms of specific clearances because our imperative here is to bring information out of the classified space as rapidly as possible and share actionable information so any—it does not matter what county or locality they are in, that they have information from DHS that is pulled generally from the intelligence community that they can act on. Our mission is to shorten that time period.

So we are working on clearances, but more importantly, we are trying to convene information-sharing fora. I mentioned the ISAC. We have all 50 States and pushing a thousand local jurisdictions. The challenge here is there are close to 10,000 election jurisdictions nationwide. so while we have what is probably the fastest-growing, most successful ISAC, we still have a pretty big gap to fill. And so we are working through what is known as—it was mentioned by Senator Warner earlier—the "last mile." We have our own last-mile initiative where we are developing tailored guidance to every single county, if they would like it, across this country. And that will include how to sign up for the ISAC, how to participate in instant response and tabletop exercises.

Senator MORAN. What is the timeframe for that to be available?

Mr. KREBS. We are marketing this aggressively now. We have already gotten four through the chute. We have 22—four States. We have 22 more States in the works right now. We have the capacity by the midterm, if every single State asks for a last mile—and it is a poster that we can share with you, and we will share it tomorrow at the closed session. It is an unclassified document. We can do all 50 States, if asked, by the midterm.

Senator MORAN. Thank you.

Chairman CRAPO. Senator Donnelly.

Senator DONNELLY. Thank you, Mr. Chairman. And thank you to the witnesses.

Mr. Krebs, have you reviewed the security of elections in Indiana specifically?

Mr. KREBS. I personally have not, but we do work with the State of Indiana, yes, sir.

Senator DONNELLY. Do you know if there are any reports in regards to your Department and what has been done in terms of hardening and securing Indiana's election for the upcoming election?

Mr. KREBS. We certainly have a profile on the State and a record of engagements and how we have engaged with the State.

Senator DONNELLY. Would that list all direct contacts between your agency and the State of Indiana?

Mr. KREBS. I am sorry. Could you repeat the question?

Senator DONNELLY. Would that list all the direct contacts that you have had back and forth, the meetings you have had?

Mr. KREBS. Yes, sir, we track the in-person engagement.

Senator DONNELLY. What I would like to do is get a copy of all of that so that we know on the State's end that we can be helpful to our State to make sure that they are getting everything they need, the last-mile program, all of these things put in place so that we have the most secure possible election, obviously in my State, but we want to have that across the country.

Mr. KREBS. We can certainly engage and provide you an update on what we are doing, particularly nationwide. But I do need to reinforce the fact that there is a level of confidentiality. Because my authorities are voluntary, I am in an entirely dependent position upon a State or a local jurisdiction to come to me and bring information and ask for help.

Senator DONNELLY. I understand.

Mr. KREBS. And if I am in a position where I am posting or sharing what is confidential information—this is just like attorney–client privilege. I am the attorney, they are the client, they own the privilege. So it is up to the partner to disclose——

Senator DONNELLY. Well, in your best judgment, you know, we would like to see what has been done to make sure that we are taking as many steps as possible in our State to secure the election.

Mr. KREBS. Yes, sir.

Senator DONNELLY. Ms. Mandelker, at the Helsinki Summit, do you know if the subject of sanctions was discussed between President Trump and Vladimir Putin?

Ms. MANDELKER. Senator, I am not aware whether or not the subject of sanctions was discussed in that very specific—in the meeting between the two of them. But I believe the President has addressed his——

Senator DONNELLY. Well, I am not asking about the President. I am asking you. Do you have any knowledge of what was discussed in that summit between the President and Vladimir Putin since you are the one who implements the very sanctions that might have been discussed?

Ms. MANDELKER. Senator, I know the President has——

Senator DONNELLY. I am asking, were you given a briefing as to what was discussed regarding sanctions in that summit meeting?

Ms. MANDELKER. Senator, we have had interagency discussions following the Helsinki——

Senator DONNELLY. Were you told what was discussed between the President and Vladimir Putin regarding sanctions? Were you given a reading as to everything that was discussed since you are the one who enforces sanctions?

Ms. MANDELKER. Senator, we have had discussions following the Helsinki Summit about what was addressed in the summit, and my mandate has been the same since the summit, which is to continue to deploy impactful sanctions——

Senator DONNELLY. Were you told whether or not the President and Vladimir Putin discussed sanctions?

Ms. MANDELKER. Again, Senator, we have had——

Senator DONNELLY. That is a simple question, yes or no. Either you were told or you were not.

Ms. MANDELKER. Again——

Senator DONNELLY. Do you know if that subject was discussed?

Ms. MANDELKER. Again, Senator, Secretary Pompeo has addressed what was discussed in Helsinki. I was not there. We have certainly had interagency discussions about the Helsinki Summit——

Senator DONNELLY. I will try one more time. This is about as simple as it gets. You can go, "Did you tie your shoe or not?" Yes or no. Did you hear whether or not sanctions were discussed in this meeting? Yes or no. Do you know if they were discussed or not?

Ms. MANDELKER. I do not know the specifics of whether or not they discussed sanctions at that meeting, but I think the President has publicly discussed his conversations with Mr. Putin——

Senator DONNELLY. But you are in charge of implementing these sanctions.

Ms. MANDELKER. What I can tell you is that, following the Helsinki Summit, my mandate remains the same, which is to continue to impose sanctions to counter Russia's malign behavior, and we have done that in full force.

Senator DONNELLY. The fact is Russia is still in Syria. They have not changed their behavior. They are still in Ukraine. They are still using cyberattacks. They are still meddling in elections. They are preparing to meddle in the upcoming elections. They are still violating the INF Treaty. This is all taking place while we have sanctions in place, which apparently have had no effect on this.

As you look at this, what sanction would have the most effect to start to turn this behavior around? And let me ask you one other question. I am running out of time here. I know we are trying to run it tight. Who do you need to get approval from to take further sanction steps?

Ms. MANDELKER. Senator, the determination——

Senator DONNELLY. There has got to be somebody.

Ms. MANDELKER. Yes, sure. Determinations about most sanctions which are either subject to Executive order or statute are made typically by the Secretary of the Treasury in consultation with the Secretary of State.

Senator DONNELLY. Has the Secretary of Treasury approved you to take any further sanctions actions you deem necessary?

Ms. MANDELKER. Absolutely. In fact, we issued sanctions just this morning in connection with Russia.

Senator DONNELLY. OK. Thank you, Mr. Chairman.

Chairman CRAPO. Senator Perdue.

Senator PERDUE. Thank you, Mr. Chairman. And thank you for your patience and forbearance this morning for being here, guys.

First of all, I want to make a comment about the closed classified briefing we had on July 31st. I must have attended a different meeting, Mr. Chairman, but I got a lot out of that meeting. There are those today who have said that we got no answers, but I think we addressed one thing in that closed briefing that I would like to touch on today, knowing that we are in an open environment.

Secretary Mandelker, first of all, let me clarify a couple things. Are you familiar with the Russian primary reserve fund that they have just closed down?

Ms. MANDELKER. Generally, Senator, but not——

Senator PERDUE. So they just closed down their primary reserve fund. They are now using their welfare reserve fund for any profits, as you say, above $70 a barrel, let us say, on the oil sector. So we are beginning to have some impact, but it has not changed behavior yet. And here is my question: With the interconnectivity of the global economy, if we put sanctions on Russia, there is a trading partner that gets hit by that as well. Today there is a study out in Germany by the Institute of World Economy that says that about 40 percent of the detriment of a sanction is borne by the trading partners across 37 countries that are dealing with Russia.

Now, that sends two messages, and I do not think either are bad. Number one, in Russia we are going to continue to do this, and trading partners of Russia, we are going to continue to do this. Is that true?

Ms. MANDELKER. I cannot verify the particular statistics, but I can tell you there is no question that when you impose sanctions in particular types of entities in Russia, those impacts affect or are felt elsewhere, and that is because of the fact that Russia is part of the global economy.

Senator PERDUE. Right, it is a global economy. Then the question is: Is it U.S. companies or is it European? Europeans are now saying that they are bearing more of the brunt because they have a higher degree of trade with Russia, and I have begun to believe that subjectively. But from a quantitative point of view, with CAATSA you have authority to do more than we are doing today. Is that true?

Ms. MANDELKER. Senator, we have—as I have already mentioned, we have issued a wide swath of designations under CAATSA, under Executive orders. We can always do more, and you are going to continue to——

Senator PERDUE. So that is the question. Let me go——

Ms. MANDELKER. ——see more from us.

Senator PERDUE. ——right there. Without getting into classified issues here, there are more things that you can do, but there is a Governor that is being used right now by someone in the Administration that says that the impact on the negative side here, the

short-term impact, we are not willing to bear that. Is that true or not?

Ms. MANDELKER. I would not say that is true, Senator. With respect to any particular designation that we issue, of course, we very closely study the impact. We want to know what the impact is going to be to U.S. businesses, to U.S. jobs, what the impact is going to be to our closest allies and partners. We also engage in a number of different discussions with those allies and partners. We study those carefully. We look to see how we can mitigate those kinds of consequences, and we make our decisions accordingly.

Senator PERDUE. But you would agree that with a larger economy like Russia, it is about a trillion-and-a-half economy. It is an entirely different equation than trying to deal with a $400 billion economy like Iran or a smaller economy like North Korea. That is a fact.

Ms. MANDELKER. I agree that those are different complex problems, yes.

Senator PERDUE. And the sanctioning regime is not an end-all. You have already said it has got to be a whole-of-Government. We have not talked enough about that today. Are you integrating with other facets of the Administration for an ultimate outcome here, and that is, a change in behavior in Russia?

Ms. MANDELKER. Absolutely, Senator.

Senator PERDUE. So what other agencies do you guys integrate with in terms of trying to change behavior in Russia?

Ms. MANDELKER. We work closely with the State Department. We work closely with the intelligence community. We work closely with the Department of Homeland Security and others.

Senator PERDUE. So, Secretary Ford, Russia has now dumped about $90 billion of U.S. Treasurys. They are doing other things to prepare for this next round of whatever sanction regime efforts that we might make.

What efforts are you aware of that Russia is trying to do to prepare? Are there things that we can do to counter that prior to the issuing of any further sanctions?

Mr. FORD. Thank you for the question, Senator. I think in an open session it is probably unwise to get too much into specifics about that.

Senator PERDUE. I understand.

Mr. FORD. You know, it is safe to assume that the Kremlin is preparing for potential future sanctions because they know full well what they intend to do and, therefore, I assume they can also anticipate that if they continue to do the kinds of things that they have done that have drawn sanctions in the past, we will continue to react to that.

Senator PERDUE. And are we in the State Department dealing with our allies, particularly our European allies who I think are bearing a higher degree of impact of this, are we in a comfortable position that they are going to stay with us, particularly when we talk about Nord Stream 2 proactively? Are we going to try to do anything to preclude that? Are the Russian allies hanging in there with us right now? And how do you project that as we get further into the sanctioning effort?

Mr. FORD. That is an ongoing piece of the diplomatic challenge. We, of course, hope that the people will hang with us in this. We think we have been doing a pretty good job of keeping the team together so far.

One example of that is the ongoing engagement that we have had with our European friends with respect to ensuring the continued rollover of sanctions against Russia for Crimea. You know, this is the kind of thing that we spend a lot of time doing.

You mentioned the issue of mitigating impact upon the U.S. economy, for example. One of the things that we did when a couple of weeks ago we issued sanctions against Russia for its chemical weapons attack in the U.K., we had a series—the most significant piece of that had to do with denial of export of national security-controlled items, a presumption of denial from the United States.

One of the carveouts that we had from that in an effort specifically to try to take into consideration the kind of concerns that you identified, sir, is a carveout for national security exports to U.S. companies operating in Russia so that we are not hurting our people operating in Russia, and we also had a carveout for Russians employed by U.S. companies in the United States, for example. So we are always mindful of those kinds of effects, and we try to mitigate them as best we can.

Senator PERDUE. Thank you, Mr. Chairman.

Chairman CRAPO. Senator Jones.

Senator JONES. Thank you, Mr. Chairman.

I would like just a real quick—it is something that I have been concerned about, and that is, I hear in the classified meetings and I hear today, and I see all of the issues that are going and all the sanctions that are being imposed and the impact, the financial impact and everything, but yet we are not hearing as much of the deterrent—the impact and the effectiveness of the deterrent. And I am curious as to just a real—if you can, has the President's comments about all this being a hoax and anything like that, is that undermining your efforts? Is Putin trying to just wait it out and hoping the President will have his way? Is that undermining your efforts?

Ms. MANDELKER. I think to the contrary, Senator. If you look at the wide range of activities that this Administration has undertaken under the direction of the President, including the very significant sanctions that we have been able to launch, including the expulsion of 60 Russians out of our country, including the closing of Russian entities in the United States, what Russia sees is a United States that is very aggressively——

Senator JONES. Yeah, but when the President is standing right next to Mr. Putin and he is just talking about hoaxes on Twitter, it just seems to undermine that. But that is OK. I understand. And I understand the response.

Mr. Krebs, I would like to ask you briefly, I know in my election in December, DHS had officials on the ground in case there were some problems. We had seen some issues with bots and other things coming up, but apparently there was not a lot of activity that day, at least as far as the Russians were concerned.

I want to kind of follow up on what Senator Tester was asking. Are you going to be able to provide that kind of support this com-

ing November for 50 States? And what kind of support would that look like? Are you focusing on specific response threats? What are we going to see from DHS on election day in November of this year?

Mr. KREBS. Thank you for the question. So, absolutely, across the 50 States, if requested, we will deploy our personnel, our field personnel—we have protective security advisers and cybersecurity advisers—across the country. They will be in the incident response cells for the State CIOs. They will also be sitting alongside the homeland security advisers. And we will deploy that again come midterms.

We just actually ran through this process last week. We had Tabletop the Vote, which was a nationwide tabletop exercise, 3-day exercise. Forty-four States plus the District of Columbia ran through scenarios, both technical hacking of election infrastructure as well as foreign information operations. And a couple takeaways from that, and just again to reinforce, when you go home, please encourage your State and local officials to work with us. But there is a need, as I mentioned, in our dependent position, we need more information as soon as it comes up. The "If you see something, say something" mantra applies here as well. We really do need State and locals to alert us as quickly and as early as possible so that we can stitch together that national picture.

So a few other things. We will be standing up, our National Cybersecurity and Communications Integration Center. We will be in kind of a war room posture that day. But we will also have a national situational awareness room where State and local officials can get on to basically a web chat, something like that, and they can share information across the country.

So, again, if they see anything, they can put it up in the situational awareness room, and they can share information visibility to get that common operating picture of our election security posture on the midterm.

Senator JONES. That is great. I want to follow up real quick with that, because you first said that if the States request it, I am assuming leading up to election day, though, there is going to be a considerable amount of information being shared. And if you are seeing something, you are going to be encouraging those States to request that information or try to do that. I mean, some States—you know, look, a lot of States are reluctant to get the Feds involved, Alabama probably one of them, you know, for a lot of reasons. But I assume there is going to be a lot of information sharing leading up to that, so you can help identify—not just relying on the States, but you can help identify where there is a particular vulnerability.

Mr. KREBS. Yes, sir, absolutely. We have every single day steady-state engagement with all 50 States and local jurisdictions. Secretary Merrill has been a partner, and we look forward to continuing to work with him. We are not just waiting for election day. The amount of progress that we have made in the last year alone is quite substantial, and we will continue pushing, pushing, pushing through the midterm. And then we will do a hot wash. We will figure out where we need to get better, and we will make that run up to the 2020 Presidential.

Senator JONES. Great. Thank you.

Thank you, Mr. Chairman.

Chairman CRAPO. Senator Tillis.

Senator TILLIS. Thank you, Mr. Chairman. Thank you all for being here and the good work you are doing.

Ms. Mandelker, or, actually, Mr. Ford, this may be in your lane, but I think one of the things that would be helpful to the Committee that could either be provided in a classified setting or ideally in an open setting so we can cut through some of the stuff that we heard today are trend lines. I am very curious to see what—let us say activities with foreign direct investment into Russia, you know, if you applied it back over some period of time, if you take a look at exits, Exxon was mentioned here. Interestingly enough, I think that JV started in the 2013–14 timeframe, probably months before Crimea was invaded, and yet for that entire period of time under the prior Administration there was not enough action to make Exxon take pause as to whether or not it made sense to do that. This Administration has.

So I think if we look at some of the economic fundamentals, movement in their GDP, the sorts of foreign direct engagement, those are going to be very helpful for us to have and kind of map that to actions that you all have taken. You may not be able to derive direct causation, but I think that that would be helpful to show, and I think we are seeing trends moving in the right direction.

I do not know if you have any information you can provide with that or whether or not that could actually be provided publicly at some point.

Ms. MANDELKER. Senator, we would be happy to provide that publicly or to you personally. There is no question that we are seeing those kinds of trend lines. There is no question that our sanctions are—the fact that we have actually gone after some of these very significant entities, oligarchs, military——

Senator TILLIS. Yeah, I would like to get that, because I would like to drill it down so that when you hear no action is being taken, no repercussions are being experienced, that seems to suggest—or to defy any logic with anybody that follows the Russian economy.

Mr. Ford, do you have anything to add to that?

Mr. FORD. Nothing to add, Senator, except that I think I would agree completely that it is very clear that Russia has been feeling pain from this. I do not have specific figures in front of me, but, of course, things like direct investment, clearly down—after we sanctioned them for the——

Senator TILLIS. Well, let us get that information, because I would really like to point to it, and we can talk more in the session tomorrow.

Mr. Krebs, do you believe that Russia started meddling in elections just in 2016 in the United States?

Mr. KREBS. Without speaking to any classified specifics, I find it hard to believe that the intelligence service has not been trying to collect information on policymakers and influence foreign outcomes.

Senator TILLIS. Do you believe it is fair to say, without sharing anything of a classified nature here, that prior Administrations would have been aware of this?

Mr. KREBS. Well, certainly the last Administration was aware, and I think before that likely——

Senator TILLIS. Do you see any evidence that internally there was any aggressive action being taken as a matter of policy or request for Congress to act to provide additional tools in that timeframe?

Mr. KREBS. So as the Under Secretary mentioned, I also was not there at that time. There is continuity of records. We have seen discussions. There were actions taken. I do think that there was perhaps a lack of appreciation at the time of the full scope of the efforts, and as you get more intelligence——

Senator TILLIS. It is easy to lay your hands on some of that that may be helpful in the closed session tomorrow, but that is not a formal request. If you can get it and it is easy, I want you to be prepared for what you intend to talk about tomorrow.

You know, the other point in relation to some questions here about burning down the Russian economy, I think that that sounds good. It may be a good sound bite. I think it is not good as a matter of strategic, precise policy where you are trying to ratchet things up without having the unintended consequences. I think, Secretary Mandelker, that is what you were trying to get to. So I think in tomorrow's session, if we could talk more about some of the matters that may not be appropriate for this setting, I would appreciate getting into that.

Mr. Krebs, in my remaining time, you mentioned that there are 22 States currently engaged that are getting into the last-mile program. Do you know whether or not or can you say whether or not North Carolina is one of them?

Mr. KREBS. Sir, I would have to circle back on that, but, again, you know, we tend to not talk about specific State engagement.

Senator TILLIS. I think the other thing that is very important, I think I heard you right by saying they have got to come and request your support.

Mr. KREBS. Yes, sir.

Senator TILLIS. So it would probably also be helpful for those of us in the Senate who want to make sure that the State is availing themselves of these resources, that we as Member of the Senate communicate to the Secretary of State or the election officials that this is a resource they should take advantage of. I would like to get your advice on how we should communicate that.

Mr. KREBS. Absolutely.

Senator TILLIS. Thank you, Mr. Chair.

Chairman CRAPO. Senator Heitkamp.

Senator HEITKAMP. Thank you, Mr. Chairman.

Mr. Krebs, I do not know if you are familiar with the story that was just out, a letter or a primary source from a young 17-year-old?

Mr. KREBS. Yes, ma'am, I did see that this morning.

Senator HEITKAMP. Very interesting reading, actually, attending a conference, a programming conference, where they were asked to try and hack into State databases and change numbers. But he decided he would do something different, and he ended up, in 5 minutes, without really knowing a lot about it, crashing the system.

You know, anyone who reads this has no confidence at all that we are headed in the right direction and that we are taking the right kind of prophylactic measures. And one of the things that we know we absolutely have to do is we have to have paper ballots.

Mr. KREBS. Yes, ma'am.

Senator HEITKAMP. So how many States have a system where they do not require paper ballots right now?

Mr. KREBS. So 5 States are entirely electronic, 14 States total have some degree of electronic nonpaper ballots.

Senator HEITKAMP. This is very problematic.

Mr. KREBS. Yes, ma'am.

Senator HEITKAMP. And I cannot say enough about the need to be very vocal in those States where they do not have paper ballots.

Mr. KREBS. As far as I have seen, every single State that does not have paper ballots is on track toward, whether at the legislative level——

Senator HEITKAMP. Will they be on track for the 2018 election?

Mr. KREBS. I do not believe so, but I think every single one of them is aiming for 2020.

Senator HEITKAMP. This is a real problem. And, you know, I am not—I was not there in the exercise. I do not know, you know, maybe in closed session we can talk a little bit about whether this experience that this young 17-year-old had is consistent with your concerns. But, you know, obviously very, very concerning and a wake-up call for all of us.

Mr. KREBS. If I can comment on that article, you know, I try to look at the glass is half-full side of this. I think with the DefCon and Black Hat conference, what we are seeing is an awakening and an awareness of the importance of security and cybersecurity in election security. That is happening. No one is sitting back and taking this on the chin. We are stepping forward. We are making progress.

I would also say that when you have—I think that individual has been in computer science for 5 or 6 years. That is also one of the greatest gaps that we have as a Nation, cybersecurity workforce, but also STEM education in our K–12 and higher education.

So when I read that article, I have some doubts——

Senator HEITKAMP. He professed that he did not have a level of skill sets that would in any way match a Russian data base or bank of hackers.

Mr. KREBS. But he is in the game, and I tell you what, that 17-year-old and the other 11-year-old that they were talking about, I want their resumes in 5 years. We need more of that.

Senator HEITKAMP. Well, I am telling you, it is a wake-up call.

Ms. Mandelker, you know, I am just going to say that I watch and we can look at all the metrics that Senator Tillis was talking about and GDP and effect. But let us get down on a microlevel because I have been watching your work regarding Rusal. It seems pretty schizophrenic. It seems not only on your side but on the tariff side where, you know, all of a sudden out of nowhere they are granted a waiver; when it becomes public, the waiver is withdrawn from their tariffs.

And so how does it really benefit us if we say we are going to give you extensions so that you can get rid of the oligarch so you can continue to function? And that seems schizophrenic to me.

Ms. MANDELKER. So, Senator, I cannot talk to the tariffs. That is a decision made by the Department of Commerce.

Senator HEITKAMP. I know that.

Ms. MANDELKER. Very specifically, with respect to Rusal, we were clear that when we designated Deripaska and his companies, we were designating those companies because they were 50 percent or more owned or controlled by Mr. Deripaska. The same was true with respect to the other oligarchs who we designated. At the same time——

Senator HEITKAMP. But you let him take his money out of the company before—then said, "We will lift the sanctions."

Ms. MANDELKER. We have not lifted any sanctions on Rusal. On the very same day that we issued those designations, we also appreciated, as we have been discussing, that those kinds of designations can have wide-ranging——

Senator HEITKAMP. Isn't that the purpose of these, to actually have wide-ranging effects that will lead to economic harm and will lead to consequences?

Ms. MANDELKER. Yes, but, Senator, with all due respect, the impact that some of those sanctions can have, Rusal was——

Senator HEITKAMP. That is true in any kind of global economy. We are going to have—no one cares that soybean farmers are collateral damage. So why do we care if other people who use aluminum are collateral damage on sanctions?

Ms. MANDELKER. So, Senator, Rusal is one of the biggest aluminum companies in the world. They have operations all over Europe. We have been in close discussions with our close partners and allies. We wanted to make sure that the impact of the designation was felt on Mr. Deripaska and not our close——

Senator HEITKAMP. I am out of time, but my only point on this is there is an approach avoidance on what you guys do, and it just seems to me that when you have your boot on the neck of a bad actor, you should keep it there.

Chairman CRAPO. Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Mr. Chairman. I thank all of you for your testimony today. And, Mr. Krebs, you have been clear that the Department of Homeland Security focuses on defense, trying to harden our infrastructure, including when it comes to elections, our election information. But I think we would all agree that even as we need to harden our defense, the best defense would be if we could deter the actions ahead of time, regardless of what they may be.

Mr. Krebs, you have talked about some of the positive signs you have seen with respect to the sanctions, and you talked primarily about other countries not engaging with the Russians when it comes to arms sales. You described it as "the dog that did not bark," right?

Mr. KREBS. I believe that was——

Senator VAN HOLLEN. I am sorry. Mr. Ford said that.

But when it comes to interference in our elections, the dogs are barking really loudly, right? I mean, we have the Director of Na-

tional Intelligence Dan Coats say the lights are flashing red. We had all of the President's top national security advisers just a few weeks ago saying that the Russians are planning to interfere or are already interfering in the 2018 elections. We have got the Microsoft story today. We have the Facebook story from a couple weeks ago.

So my question to you as an experienced diplomat, who is Putin listening to? Is he listening to DNI Coats or is he listening to what President Trump is saying in Helsinki and at the rally 24 hours after all those national security advisers met saying that this is "a Russian hoax"? Who is President Putin listening to?

Mr. FORD. I guess I will venture to take that one, Senator.

Senator VAN HOLLEN. That is, I am sorry, Mr. Ford, for you.

Mr. FORD. I am obviously not in a position to describe in any useful detail, you know, to whom President Putin is listening in his own inner councils. I certainly hope someone knows that, but I do not know myself. I can say that my own impression from these issues has been that the Russians are very well aware of what in the Soviet era they used to call "the correlation of forces." They understand what it means to feel pain and what it is for economic and other sanctions—other factors to play together in a country's national power.

What we are trying to do, putting aside whatever it is—I understand your question, but I think from a Russian perspective, my guess would be that they are very attuned to the net impact we are having upon their ability to project power into——

Senator VAN HOLLEN. Mr. Ford, I am asking about the elections. We have evidence, including this morning, that they clearly have not gotten the message with respect to interfering in our politics, in our elections. You said earlier that the obvious objective is to influence Russian behavior. That is the obvious objective of sanctions. You also said that we need to make it clear that there will be a painful result if the Russians engage in malign behavior.

Here is what Secretary Pompeo said in response to a question from Senator Rubio just a few weeks ago in the Senate Foreign Relations Committee, because Senator Rubio and I have introduced the DETER Act, which would establish very clear, certain penalties on Russian behavior if we catch them again interfering in our elections.

Secretary Pompeo said, "Senator, I completely agree with you that there is a cost-benefit calculation that is undertaken before the Russians act. So it follows necessarily that putting them on notice with essentially a fail-safe about things that will follow has the likelihood of being successful in raising the cost in terms of how he calculates risks associated with a wide range of actions."

Do you agree with the Secretary's statement?

Mr. FORD. I clearly agree with Secretary Pompeo. I think it is important—as I was explaining a bit earlier, I think it is important to protect and advance a couple different equities simultaneously here. We need to influence Russian behavior. In the sanctions context, we need to protect the economic and competitive interests and job equities that we have. We need to protect our relationships with other players around the world.

We do not have, to my knowledge, an interagency position on that particular piece of legislation at this time. I believe it presents

challenges from the perspective of the degree to which we are in—the degree to which it is possible to have a national security waiver. As part of——

Senator VAN HOLLEN. Mr. Ford, I am sorry. My time is running out, and we can work on issues regarding a waiver.

Mr. FORD. We would be happy to engage in all these questions.

Senator VAN HOLLEN. But I worried a little bit when you said they can study to the test. The reality is under the DETER Act, there is no getting around the penalties, right? That is the whole idea of deterrence. You have clear, harsh penalties. And I should stress these are contingent penalties. We have had a lot of talk about whether we should increase sanctions on Russia today. What we are talking about in this piece of legislation is if they get caught interfering in our elections in 2018, after this bill were to pass, then there would be harsh sanctions. Do you agree with the Secretary that that seems like a good framework to approach this issue?

Mr. FORD. We have already made very clear that, you know, there are behaviors—and that is one of them—that would be unacceptable, and we certainly plan and would expect to make Russia regret any step of that sort. We would be happy to work with you and your staff to provide input to make sure that this legislation, if it moves forward, is as well crafted as it can be, including from the perspective of making sure that this is not a blunderbuss but more of a rapier or rheostat that we can use as a tool of diplomacy and behavioral inducement to help ensure that Russia behaves better and that we can modulate pressures in response to how their behavior——

Senator VAN HOLLEN. Well, thank you. That was a lot of adjectives, but the point—today we know that they are not getting the message. I mean, we know that, right? You do not have to tell us. The Director of National Intelligence and everybody has told us that they clearly are not getting the message today, despite what you and everybody else has been saying.

So we have got about 80 days, less than that, to go, and my goodness, if we cannot come up with a way to safeguard the integrity of our democracy in the next 80 days, shame on us.

Chairman CRAPO. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you.

Let me try a different tactic. Let me ask the three of you if you can help me understand the Administration's strategy toward Russia's election interference. What theory of behavioral change is the Administration pursuing that entails Treasury designating a series of Russian entities and individuals on the one hand, and has President Trump standing next to Putin and saying Russia is not targeting U.S. elections on the other? What is the thinking that links those two actions? Can any of you answer that?

Ms. MANDELKER. Senator, I think the President later corrected what he had said during that press conference. But the bottom line is that we have been——

Senator CORTEZ MASTO. And are you getting clear direction from the President in addressing the concern that I am hearing from all of my colleagues in a bipartisan manner to address what Russia is doing in interfering with our election process?

Ms. MANDELKER. Absolutely, Senator.

Senator CORTEZ MASTO. So what additional sanctions can Treasury impose?

Ms. MANDELKER. Again, this morning we imposed additional sanctions. It is a very active program for us. As I have already mentioned, we have designated some of the biggest companies in Russia. We have designated some of Putin's closest allies who have an enormous amount of wealth, which was seriously impacted by our sanctions. The impact of our sanctions has also had a worldwide impact for Russia. It has had a chilling effect on individuals and companies and countries who are considering doing business with Russia because they understand that——

Senator CORTEZ MASTO. Well, Ms. Mandelker, I only have so much time. Let me ask, because I know——

Ms. MANDELKER. ——there are always more to come from the Treasury Department.

Senator CORTEZ MASTO. I appreciate that, and we have had this conversation in the confidential briefing as well, which I was not impressed with.

There is evidence through the Panama Papers or *Russian Forbes* suggesting that several childhood friends of President Putin have come into enormous financial windfalls that raise strong suspicions of corruption. These men are just a few of the Russian individuals and entities that experts have suggested should be designated under CAATSA authority. Does Treasury have the authority under CAATSA to pursue these individuals? And are you pursuing them?

Ms. MANDELKER. I cannot speak to any particular individuals without knowing their names and circumstances, but, absolutely, we have very broad——

Senator CORTEZ MASTO. So you are not aware of those individuals and the evidence through the Panama Papers or the *Russian Forbes*? You are not familiar with what I am talking about?

Ms. MANDELKER. Senator, as you are aware, we have conducted with the interagency a very extensive report under CAATSA which detailed a number of oligarchs and senior foreign officials who are close to Putin. We have a great deal of information about those individuals, and we have designated a number of them.

Senator CORTEZ MASTO. So my colleague just referred to the DETER Act. Do you support it?

Ms. MANDELKER. Senator, I know the Administration is happy to work with the Senate on the DETER Act or any other particular piece of legislation——

Senator CORTEZ MASTO. Is there any language in the DETER Act that you have concerns about?

Ms. MANDELKER. We are happy to sit down and provide that kind of guidance. I think those discussions have already been well underway.

Senator CORTEZ MASTO. Mr. Krebs, you identified there were five States without paper ballots. Are you currently working with those States to shore up the integrity of their election?

Mr. KREBS. Yes, ma'am. We work with all 50 States.

Senator CORTEZ MASTO. And you are currently working with those five?

Mr. KREBS. Yes, ma'am.

Senator CORTEZ MASTO. Is there anything that we can do in Congress to continue to support shoring up the election integrity in all of those States and what you are doing in working with them?

Mr. KREBS. Absolutely. I think I have already mentioned that when you do go back to your jurisdictions, when you go back to your districts, please encourage your State and local officials to work with us. You know, we hit them up every day, but I think the more voices they hear—you know, I do not want to undersell the level of work and partnership we are seeing, but we can always do more.

Senator CORTEZ MASTO. So there was an opportunity to supply—appropriate $250 million to the States, on top of the $380 million that was appropriated for the States that the States have utilized. Are you hearing from those States that additional dollars, the $250 million, would have been helpful to help shore up the integrity of the election process?

Mr. KREBS. As I understand it, they are in the process of implementing that $380 million, which was a much-needed infusion. Going forward, there will be a requirement for additional funding. What we are trying to help States with is refine what the ask is and really get to the bottom of what is it that they need and how are they going to use it.

There have been investments at the State level because ultimately this is a State and local responsibility to administer Federal elections. We are in a supporting role. The question going forward is: Is there money needed? How much? Where is it going to come from? And then how are going to—if it is a Federal spend, how are we going to ensure the appropriate risk-based security outcome?

Senator CORTEZ MASTO. And besides paper ballots, is there anything else that can be——

Mr. KREBS. Auditability, yes, ma'am. Auditability.

Senator CORTEZ MASTO. OK. Thank you. I know my time is running out. Thank you very much.

Chairman CRAPO. Thank you.

Senator Warren.

Senator WARREN. Thank you, Mr. Chairman.

Sanctions usually involve an effort to follow the money, and Russians close to Putin are using every opportunity they can to make it harder for the United States to follow the money. The recent defense bill requires Treasury to brief Congress on the assets owned by Vladimir Putin and his cronies, including the location, value, size, and contents of their bank accounts, real estate holdings, and all other financial assets, and the shell companies they use to hide those assets. That bill has now been signed into law.

Under Secretary Mandelker, when can we expect you to provide this briefing?

Ms. MANDELKER. Senator, we would be happy to work with your staff on this briefing. What I can also tell you——

Senator WARREN. This is not about working with my staff. You are supposed to give a briefing to all of Congress. I just want to know when it will be ready.

Ms. MANDELKER. I cannot give you a date, but I am happy to get back to you on that. I am happy to give you that briefing.

Senator WARREN. Weeks? Months?

Ms. MANDELKER. Again, Senator, I believe that that requirement was that we conduct that briefing in consultation with the Director of National Intelligence and the State Department——

Senator WARREN. Have you started that?

Ms. MANDELKER. ——and we will—we have a number of efforts underway. In fact, we detailed——

Senator WARREN. Is that a yes or a no?

Ms. MANDELKER. Again, Senator, we have a number of efforts underway to follow the money. We just provided an extensive report to Congress pursuant to CAATSA, and——

Senator WARREN. Well, you know, you have a requirement here in the law, and I am just asking about one thing, about a report you are supposed to produce, and I just want to know when you are going to produce the report. I ask this question because, frankly, I am not convinced that Treasury is doing everything possible to hold Putin accountable for using cyberattacks to interfere in our elections and those of our allies, for illegally occupying Ukraine, for propping up Syrian dictator Assad.

Congress required Treasury to provide a report on the net worth and income sources of senior Russians close to Putin, and instead, I saw what you did. You copied and pasted the *Forbes* billionaires list. Thank you, but we already had that.

The Senate Intelligence Committee asked Treasury to help follow the trail of dirty Russian money to investigate Russia's interference in our election, and you are reportedly dragging your feet on that. It has been over a year since Congress overwhelmingly passed sanctions on Russia. You still have not implemented seven mandatory provisions of that law.

It is not hard to see why Putin thinks he can still interfere in our elections and get away with it. The American people and the world deserve to know how Putin makes his money, and if we want to squeeze Putin and his cronies, we need to follow the money and expose those assets so that these corrupt individuals have fewer ways to ignore the sanctions.

So I want to ask you another question, following up on what Senator Heitkamp asked. Last month, just says after President Trump met with President Putin in Finland, Rusal, this sanctioned Russian aluminum company controlled by a sanctioned Putin crony, received an exemption from President Trump's tariffs in the Commerce Department. Treasury reportedly signed off on this exemption. I sent a letter to the Commerce Department asking questions about the decision, and 1 day later, the Administration reversed its tariff exemption. I was very glad to see that. But can you tell me—I still have a simple question. How did Treasury allow a tariff exemption for the subsidiary of a sanctioned Russian company in the first place, given that the tariff was meant to protect American suppliers?

Ms. MANDELKER. Senator, that was a decision by the Department of Commerce, not a decision by the Treasury Department. That is not a decision——

Senator WARREN. And so the information that you signed off on it and then reversed positions is not accurate?

Ms. MANDELKER. That is right, Senator.

Senator WARREN. OK. You are saying it did not—it is not accurate that that did not happen. All right. So let me ask the rest of it. Meanwhile, Treasury is reportedly considering lifting sanctions on Rusal, which is sanctioned for its financial ties to a corrupt Russian oligarch who contributed to Putin's illegal occupation of Ukraine. Treasury Secretary Mnuchin recently said he was concerned about "the hardworking people of Rusal."

So let me ask, has Putin withdrawn from the illegal occupation of Ukraine, stopped cyberattacks and disinformation, or halted efforts to spread corruption?

Ms. MANDELKER. Senator, I just want to correct one point from your earlier question.

Senator WARREN. Yes?

Ms. MANDELKER. The oligarch report, the classified oligarch report, as we have said repeatedly, was a very extensive piece of work. It involved over 2,500 hours of work within the interagency. So in terms of following the money, we have undertaken——

Senator WARREN. Well, look, I am now out of time——

Ms. MANDELKER. ——not just in that report but in a number——

Senator WARREN. ——but let me just say on this, we just passed a law about this. I just asked you about when you—asking you for a report, and it was signed into law, and all I ask you is when are you going to follow that, and you tell me, "We already have." If we thought you had already done it, we would not have passed another law asking for this report. So I think it is perfectly fair to ask you when you are going to comply with the law that President Trump recently signed in effect?

Ms. MANDELKER. And, again, Senator, I have made clear that that law requires that we provide a briefing. We are happy to do that. We just provided a report last week——

Senator WARREN. When? That was my question.

Ms. MANDELKER. ——covering illicit finance of money laundering by Russia.

Senator WARREN. And when are you ready for that briefing?

Ms. MANDELKER. Excuse me.

Senator WARREN. When? That was my question. That was the whole question. It was a short question.

Ms. MANDELKER. I understand. We are happy to get back to you. That is a briefing that we would do with the Director of National Intelligence and the State Department. I am not prepared to give you a date today, but we will give you a date in short order.

Senator WARREN. Or even a ball park. Thank you.

Chairman CRAPO. Senator Reed.

Senator REED. Well, thank you, Mr. Chairman.

Let me ask if anyone would disagree with the statement that we have irrefutable, uncontradicted evidence that the Russian Government, at the direction of President Putin, interfered in the 2016 election to favor the candidacy of President Trump and disfavor the candidacy of Secretary Clinton, that they continue to engage in activities to undermine our election process throughout the United States? Does anyone disagree with that?

Mr. KREBS. Sir, I think that tracks against the intelligence community's assessment——

Senator REED. That is a fact. So, again, going back to questions that Senator Jones and Senator Van Hollen raised, why does the President seem unwilling to accept this fact? As recently as yesterday, he suggested that it may or may not have been the Russians in an interview with Reuters. Why doesn't he accept what is the facts?

Mr. KREBS. Sir, I believe he has supported the intelligence community. He supports the intelligence community. As Under Secretary Mandelker said, he clarified his statement on the Tuesday after. Just a couple weeks ago in New York City, Vice President Pence was very emphatic about supporting the intelligence community and that protecting our elections is a priority.

Senator REED. So why yesterday when he is asked about the Mueller investigation, he criticizes it, says it plays right into the hands of Russians, if it was the Russians?

Mr. KREBS. Sir, I am not aware of that report. Again, I——

Senator REED. Well, it was in the newspaper today.

Mr. KREBS. So the President has been clear he supports the intelligence community. I have all the guidance, the direction, and the authorities that I need to help State and local election officials.

Senator REED. Would it help your efforts if the President of the United States, your efforts both nationally and internationally, if the President of the United States made a statement to the American people that essentially reaffirmed the statement I just made, i.e., we were attacked by the Russians at the direction of Putin, it was designed to affect the election in 2016, they are continuing to attack us? Would that help your efforts in terms of bolstering election security if the President actually said that directly rather than every other day equivocating?

Mr. KREBS. Again, sir, the President supports the intelligence community assessment. He has said that publicly. I have what I need to——

Senator REED. Well, then why does he turn around and say, "I support the intelligence community assessment," but just as recently as yesterday saying, "Well, it may be the Russians, maybe not"? How does that support the intelligence community assessment when the intelligence community assessment, as you have all conceded, is absolutely conclusive as to the involvement of Russia at the direction of Putin, and their continuing ongoing threat to the United States? I mean, this is as if a previous President sort of said, "Well, you know, we were attacked, but it could have been those guys or maybe somebody else." I do not think that is the way our previous Presidents have acted. I do not think you have an answer.

Mr. KREBS. Sir, again, I have the guidance I need to go and engage.

Senator REED. But what about engaging the American people and the international community? They are looking at, as my colleagues have suggested, questions of, well, the President does not really believe that. One of the issues that is coming up shortly is that the European Union every 6 months has to renew sanctions. That expires January 31st of 2019. Is there a chance that one—and it has to be unanimous—that one of those countries could say, you

know, "This is no big deal with the President, I mean, we do not have to do that"?

Ms. MANDELKER. Senator, we engage very extensively with our European colleagues precisely on those sanctions. They just issued additional sanctions at the end of last month that followed sanctions that we had previously designated. We are going to continue to work with our colleagues in the EU to have them continue to ratchet up the pressure that we have already been placing on the Russian economy. Those discussions have been quite productive.

Senator REED. So have you heard any of your European colleagues suggest to you that they are confused about the President's statements?

Ms. MANDELKER. No, Senator.

Senator REED. So they are as completely assured of his situation as we are? And, frankly, you cannot explain the comment yesterday. Neither can I. Why would one question whether the Russians are involved in the election as recently as yesterday if, in fact, you do support the intelligence community?

Thank you.

Chairman CRAPO. Thank you, Senator Reed, and that concludes the questioning.

Questions submitted by Senators will be due by next Tuesday, and I ask all of our witnesses to respond promptly to those questions if they are submitted to them.

And with that, this hearing is concluded. Thank you again for your attendance and willingness to share your expertise with us here today. Thank you.

[Whereupon, at 12:14 p.m., the hearing was adjourned.]

[Prepared statements and responses to written questions supplied for the record follow:]

## PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

This morning the Committee will receive testimony from senior Administration officials from the Departments of Treasury, State, and Homeland Security on the implementation and effectiveness of the sanctions program currently in place against Russia.

The reasons for these sanctions include Russia's standing military incursions in Ukraine; abetting Assad's atrocities in Syria; conducting cyberenabled information warfare activities and cyberattacks against United States critical infrastructure, including its malicious meddling in U.S. elections, among a host of other malign Russian activities.

The Banking Committee plays a leading role in developing any legislation that proposes the use of sanctions and financial pressure, more especially those measures involving financial institutions, sovereign debt, and other financial instruments to address serious threats to the national security of the United States.

Just about 1 year ago, on August 2nd, the President signed into law the Countering America's Adversaries Through Sanctions Act of 2017, known as CAATSA, which included in it, among other things, authorities for not only a set of strengthened sanctions against Russia but also brand new authorities for several powerful mandatory secondary sanctions.

It was this Committee that put together the foundation for those sanctions and financial measures on Russia and then worked with the Committee on Foreign Relations to expand them as part of CAATSA.

CAATSA was truly a four-square effort: it was not only strongly bipartisan but also bicameral. It passed the House by a vote of 419–3 and two days later, by the Senate on a 98–2 vote.

It's not often that Congress acts together in such a strong manner, as marked by such near-unanimous votes. But, then, Russia is a menace on so many different levels, today, that Congress can be compelled to act with a single voice to find solutions that will protect America and democratic values across the world.

To its credit, the Administration, in the year since CAATSA, has imposed some of the toughest sanctions in years on Russia, particularly with regard to those imposed in April on Russia's oligarchs and their business associations.

The bulk of sanctions imposed against Russia pertain to its unlawful invasion and annexation of Crimea. These were strengthened by Congress in CAATSA and absent any change in Putin's behavior, will likely remain in place until he's no longer in power and Crimea is returned.

In all, over the last year, the Administration has sanctioned over 200 targeted Russian individuals and entities, for either its cyberattacks or Ukraine behavior either pursuant to congressional sanctions, or under its own executive authority.

I hope to receive an update today from our witnesses on how the sanctions against Russia are being implemented and enforced.

It was a positive step when, 2 weeks ago, in response to Russia's use of a nerve agent in Britain against one of its former spies and his daughter, the State Department showed its resolve against Moscow while it took a stand with our British allies by imposing a set of escalatory sanctions under the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991.

The Administration is taking some important steps against Putin, his cronies, and the industrial apparatus they control, but can Congress expect more from the Administration—and, when?

Congress itself is positioned to do more. There are bills in this Committee and in the Foreign Relations committee which seek to escalate economic pain throughout Russia's banking and energy sectors and sovereign debt markets.

As we all, and that includes the Administration, consider next steps to further constrain Putin, including sanctions and other diplomatic initiatives, several questions come to mind——

What degree of success have the existing evolutions of sanctions, which work to constrain the Russian economy and derail the activities of those individuals closest to Putin, had on Putin's behavior at home and abroad?

What is the most effective way to coordinate and strengthen sanctions with our European allies and other partners?

---

## PREPARED STATEMENT OF SENATOR SHERROD BROWN

Mr. Chairman, thank you for agreeing to this important hearing, the first in a series in the coming weeks on sanctions and other measures that might more forcefully counter Russia's continuing efforts to attack the U.S. and our allies.

While sanctions have had some effect on Russia's economy, it's not clear what effect they have had on Russia's malign activities around the world. Russia remains in Crimea, its proxies are still in eastern Ukraine, it serves as the arsenal of Assad, and it continues to attack our electoral system and other key components of our infrastructure.

We must send a more powerful and direct message to Putin and those within his circles: We know what you're doing, it must stop, and if you continue, you and your Government will pay a dear price.

Over a year ago, Congress gave the President the authority to use more assertive sanctions against Russia.

My colleagues and I have pressed for nearly a year for stronger CAATSA implementation. After months of waiting, we requested assessments by the Inspectors General of the Intelligence Community, State, and Treasury Departments.

These hearings, and these IG audits, are not simply a reaction to the President's startling performance in Helsinki, which was widely panned on both sides of the aisle and the Atlantic. There is a deeper problem. With a few exceptions, the President has refused to use the new authorities under CAATSA.

Let me give you one example. Administration officials identified Russians responsible for supplying chemical weapons components for use in Syria, the ones that killed and maimed men, women, and children alike. Our U.N. Ambassador announced the imminent imposition of sanctions. The next day they were withdrawn, reportedly on orders from the President.

That is not the way mandatory sanctions operate. Section 231 of CAATSA requires that once violators are identified, they must be sanctioned, or waivers exercised—these defense and intelligence sanctions in CAATSA were not permissive, they were mandatory. And then the Administration requested that a broader waiver to section 231 be included in the defense bill last month, basically because the President could not certify the key condition of the existing waiver: that Russia was significantly reducing its cyberattacks against the United States.

I think it was a bad idea to use the recent defense bill to relax waiver authorities on Russian defense and intelligence sector sanctions, and then effectively exempt those waivers from Congressional review under CAATSA. Instead of strengthening sanctions, we've gone in the opposite direction. We should be strengthening, not weakening, sanctions.

And that's why the Administration continues to face fierce bipartisan criticism on its Russia policy, why a new round of oversight hearings is being convened, and why members on both sides are proposing new sanctions.

In addition to urging the Administration to use CAATSA as it was intended, I think most of us agree Congress should also do more to increase pressure. Congress crafted tough, comprehensive Russia sanctions, enacted last August by overwhelming majorities in both chambers—419–3 in the House, 98–2 in the Senate. We should build on that broad bipartisan consensus.

We should focus on the facts and broader strategic questions: What is Russia's Government still doing in Syria, Ukraine and Crimea? What active cyberattacks are they directing against our elections and critical infrastructure? And what powerful economic, trade, financial, diplomatic and political tools can we deploy now to deter those threats—or threaten to deploy by dropping the hammer if they continue?

Russia's election interference, confirmed unanimously by U.S. intelligence earlier this year, and reaffirmed since then, poses a problem that goes far beyond foreign policy, and strikes at the core of our democracy. This is not a partisan issue. There is no disagreement about what happened here.

Now we're less than 100 days away from another election, and the Director of National Intelligence has been sounding the alarm that the warning lights are blinking red again.

And while some efforts are being made to bolster State election security measures, and otherwise contain these threats, including a markup of a measure this week in Rules, it appears little is being done to address their source: Russia's Government.

I know my constituents are clear-eyed about these threats. The Ukrainian community in Ohio and around the world knows firsthand—like our NATO allies Latvia, Lithuania, Estonia—the dangers of unchecked Russian aggression.

I also know, as past Committee witnesses have said, U.S./EU unity is critical if sanctions on Russia are to be effective.

That's why we should not only press to more aggressively implement current Russian sanctions, but we must also strengthen our response. New bipartisan sanctions measures have been introduced. These hearings are a critical next step.

Today we're joined by Treasury Under Secretary Mandelker; Assistant Secretary for International Security and Non-Proliferation Chris Ford from the Department of State; and Christopher Krebs, Under Secretary for the National Protection and Pro-

grams Directorate, Department of Homeland Security—three people responsible for policy on countering Russia within the Administration. I welcome you all. I am interested to hear your perspective on where we are, what effects the current sanctions regime is having on Russia's economy and behavior, and where you think we're headed in the coming months.

---

## PREPARED STATEMENT OF SIGAL P. MANDELKER

UNDER SECRETARY, TERRORISM AND FINANCIAL INTELLIGENCE, AND ACTING DEPUTY SECRETARY, DEPARTMENT OF THE TREASURY

AUGUST 21, 2018

**Treasury's Efforts To Counter Russian Malign Activity**

Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee, thank you for inviting me here today to speak on behalf of the Treasury Department and provide an update on our comprehensive efforts to counter Russia's malign activity. Our efforts, taken together with our partners across the U.S. Government and around the world, are guided by a clear understanding of the threat Russia poses to the United States and to our friends and allies.

As Russia seeks to challenge the United States and its allies, we see this threat manifest itself in a variety of ways, including by: continuing its occupation of Crimea and ongoing aggression against Ukraine, attempting to subvert Western democracies, including our own, through election interference; enabling the Assad regime's massacres in Syria; using chemical weapons in an attempt to assassinate a British citizen and his daughter in the United Kingdom; perpetrating malicious cyberattacks; maintaining ties to transnational organized criminal groups; violating human rights at home; fostering corruption across Russia's economy; and facilitating sanctions evasion and other illicit activity across the globe. The breadth and brazenness of Russia's malign conduct demands a firm and vigorous response.

Precisely for this reason, Treasury's Russia sanctions program is among our most active and impactful. Since January 2017, this Administration has sanctioned 217 Russian-related individuals and entities for a broad range of activities, 200 of which were sanctioned by Treasury's Office of Foreign Assets Control (OFAC). Indeed, we have issued Russia-related measures in 7 of the last 9 months. Since the start of this Administration, Treasury has also added 32 Russian entities to its Sectoral Sanctions Identification List, subjecting those listed to debt and equity restrictions, as well as prohibitions on the provision of goods, services, and technology in support of certain energy projects in Russia. Pursuant to the Countering America's Adversaries Through Sanctions Act (CAATSA), we have also tightened these restrictions.

In doing so we have targeted a veritable "who's who" of Russia's most prominent companies. These include Rosoboronexport, Russia's primary State-owned weapons trading company; EuroSibEnergo, among the largest independent power companies in Russia; and Surgutneftegaz, a major Russian oil company.

Our targets also include the heads of major State-owned banks and energy firms, as well as some of Putin's closest associates. These figures include Putin affiliates Oleg Deripaska and Viktor Vekselberg; Putin's current or former son in law Kirill Shamalov; the heads of State-owned companies such as Gazprom's Alexei Miller, Gazprombank's Andrey Akimov, and VTB Bank's Andre Kostin; the head of the Russian Security Council, Nikolai Patrushev; and the Russian Minister of Interior, Vladimir Kolokoltsev. Dealings with such persons on our Specially Designated Nationals and Blocked Persons List, moreover, create exposure to secondary sanctions under CAATSA, meaning that persons who deal with them risk being sanctioned themselves. Targeting these Russian individuals and entities have made them radioactive, as we have made clear to the world that those who choose to continue to do business with them do so at their own peril.

That CAATSA was passed by a near unanimous vote demonstrated great resolve by Congress to counter Russia's malign activity. We share that resolve. The Department of the Treasury's approach towards Russia is informed by this Administration's 2018 National Security Strategy, which clearly recognizes the full range of Russian malign activity, and which prioritizes the importance of economic tools to "deter, coerce, and constrain" our adversaries.

As companies across the globe work to distance themselves from sanctioned Russian persons, our actions are imposing an unprecedented level of financial pressure on those supporting the Kremlin's malign agenda and on key sectors of the Russian economy.

Treasury's actions have caused extensive consequences to the financial interests of targeted individuals and entities, including blocking hundreds of millions of dol-

lars in Russian assets in the United States. Targeted State-owned banks and other sanctioned entities likely have higher financing costs than they otherwise would if not for Treasury's prohibitions on debt purchases. Russian companies designated for their links to Crimea have been forced to cut production and have lost business relationships with foreign commercial partners. In addition, we have cut off, from the U.S. financial system and beyond, malicious cyberactors, including those providing offensive cybercapabilities to the Russian intelligence services, some of whom covertly worked on behalf of the Kremlin to interfere with the 2016 U.S. election. Such reactions illustrate the substantial costs our measures are imposing on those who undermine U.S. interests.

Building on sanctions implemented since 2014, the impacts of our Russia-related sanctions are felt far beyond the targeted entities and persons. Western sanctions and subsequent geopolitical tensions have raised uncertainty and dampened domestic and foreign private investment in Russia. In the energy sector, our sanctions have limited important investment in exploratory energy projects needed to help grow Russia's oil and gas production capacity. Overall foreign direct investment into Russia has fallen over 5 percent since 2013, with sizeable declines in direct investments from the United States, which have fallen 80 percent since 2013. Direct investment into Russia from other major economies also declined over the same period. Russia is taking note of these impacts.

In addition to sanctions, we are also strategically and smartly deploying Treasury's other economic authorities—such as anti– money laundering (AML) measures, enforcement actions, actions under Section 311 of the USA PATRIOT Act, foreign engagement, and private sector partnerships, among other tools—to disrupt Russia's illicit financial conduct and harden the international financial system against its predation. We are directly engaging our foreign allies and partners, especially those in Europe, to coordinate these efforts and augment the impact of our actions. We are working closely with our interagency partners to deploy the full range of other financial, intelligence, law enforcement, and diplomatic tools to expose, disrupt, and impose costs on those responsible for Russia's malign activities.

By strategically leveraging all of these complementary authorities, we are increasing financial pressure on Russia to advance our national security priorities while simultaneously mitigating unnecessary impacts on the United States, our European allies, and the global economy. We recently submitted a report pursuant to Section 243 of CAATSA further elaborating on these efforts (see Attachment).

We have imposed major costs on Russia. Yet the significance of our actions and other financial measures must ultimately be measured in terms of their strategic impacts. Though Russia's malign activities continue, we believe its adventurism undoubtedly has been checked by the knowledge that we can bring much more economic pain to bear using our powerful range of authorities—and that we will not hesitate to do so if its conduct does not demonstrably and significantly change.

**Overview and Impact of April 6 Oligarch and Russian Official Designations**

An important example of the impact that Treasury actions have had on Russia was in our April 6, 2018, designation of 38 entities and individuals, including 7 Russian oligarchs and 12 companies they own or control, and a major State-owned Russian weapons trading company and its bank subsidiary. This action included sanctions against 17 senior Russian Government officials, many of whom were appointed to their posts by Putin and hold prominent positions in the Russian Government and business community.

Among the 12 companies sanctioned are Renova Group, an international group of asset management companies and investment funds owned by Vekselberg; RUSAL, the second-largest producer of aluminum in the world; EN+, a publicly traded holding company for Deripaska's metals and energy assets; GAZ Group, Russia's leading producer of commercial vehicles; and EuroSibEnergo, as mentioned above, one of Russia's largest independent power companies.

As a result of this action, we have impeded the ability of these actors to access the financial system, reduced the value of their assets, and forced companies to extricate themselves from involvement with designated actors. Other tangible impacts include:

- Since being designated, Deripaska's estimated net worth has dropped by roughly 50 percent, and the share price of EN+ fell from $12.20 to $5.40 on the London Stock Exchange following its designation.
- Vekselberg's net worth dropped an estimated $3 billion, and foreign Governments have launched investigations and frozen Vekselberg's assets in their jurisdictions. Additionally, Vekselberg's Renova Group was forced to divest from ventures in Switzerland and Italy.

As our public actions continue to draw high-profile attention to those individuals and entities charged with carrying out Putin's orders, the world takes note. Many have become pariahs in the international community and have lost their ability to portray themselves as legitimate businessmen.

**Additional Treasury Actions**

We have also targeted Russia's malicious cyberactivity, sanctioning those behind Russia's interference in the 2016 U.S. election, as well as companies developing and procuring offensive cybercapabilities and underwater technologies for the Federal Security Service (FSB). We designated two Russian intelligence organizations—FSB and the Main Intelligence Directorate (GRU)—both of which engage in activities that undermine U.S. cybersecurity on behalf of the Russian Government.

In March, we designated Russian oligarch Yevgeniy Viktorovich Prigozhin under our cyberauthorities for funding the operations of the Internet Research Agency, which has covertly worked on behalf of the Kremlin to influence social media networks and interfere with the 2016 U.S. election. In exposing the activities of these organizations and designating companies for their dealings with them, we not only cut them off from the United States and U.S. persons, but subject third parties who deal with them to potential sanctions as well.

We also are exposing and disrupting Russian support to rogue States. We used our Syria authorities to sanction Russia's primary State-owned defense firm and its bank subsidiary for supplying Russian military equipment to the Assad regime, hindering the firm's ability to receive payments from existing contracts with other countries. And just earlier this month, we designated a Russian bank, Agrosoyuz Commercial Bank, for knowingly facilitating a significant transaction on behalf of U.S. and U.N.-designated North Korean individuals and entities.

Our sanctions have blocked hundreds of millions of dollars in Russian assets in the United States and caused extensive damage to the economic interests of affected individuals and entities. Companies and individuals around the world have cut ties to sanctioned actors in attempts to protect their commercial interests. Notably, in early 2018, Exxon announced that it had decided to end its joint exploration ventures with Rosneft due to the continued economic pressure imposed by our sanctions. In 2017, Rosneft separately announced a hold on a major South Black Sea project, citing sanctions as limiting its ability to obtain modem technology and equipment.

We also continue to track and target illicit financial hubs where Russian actors try to hide their money. Earlier this year, we used our authorities under Section 311 of the USA PATRIOT Act to find Latvian-based ABLV Bank to be a foreign financial institution of primary money laundering concern, proposing to prohibit U.S. financial institutions from maintaining correspondent accounts on behalf of the bank. In this finding and proposed rulemaking, FinCEN cited multiple instances of institutionalized money laundering in which ABLV management solicited high-risk shell company activity that enabled the bank and—its customers to launder funds. ABLV's facilitation of shell company activity typically benefited illicit actors engaged in an array of illicit conduct, including transnational organized criminal activity, corruption, and sanctions evasion, including activity emanating from Russia. This finding and proposed action not only was a shock to the Latvian banking system, helping prompt that country to undertake certain reforms, but it also put financial institutions in other similar financial hubs on notice that we will not hesitate to act against banks that institutionalize money laundering as a pillar of their business practice.

**TFI's Work To Advance Our National Security**

In the Office of Terrorism and Financial Intelligence (TFI), I work with some of the most dedicated professionals in the U.S. Government, who are working countless hours to implement programs that protect our national security. This is especially true when it comes to our Russia team, who are wholly committed to the mission.

In addition to our robust Russia program, we also have teams of people working across a wide spectrum of other programs. Under this Administration, Treasury has sanctioned more than 1,300 individuals, entities, vessels, and aircraft.

In order for us to implement all of these programs and maximize the effectiveness of our financial tools, Treasury also has spent significant resources drafting new Executive Orders, issuing advisories, and providing guidance such as Frequently Asked Questions to the public and private sector. Our team also travels around the world to ensure our sanctions are effectively implemented and the real-world risks of transacting with designated individuals and entities are fully understood.

Here in Washington, our staff fields thousands of inquiries regarding compliance and licensing issues—many highly complicated questions that require substantial

amounts of time, expertise, and effort. Since the start of FY2018, OFAC has received nearly 50,000 phone calls for guidance on our sanctions programs, including our various Russia-related authorities. On top of this, we are required to prepare and submit at least 80 reports to Congress in 2018—reports that require thousands of hours of work. To highlight just one example, the classified oligarch report required by Section 241 of CAATSA encompassed more than 2,500 hours of interagency work over the course of several months.

TFI and the interagency colleagues with whom we work bring this same dedication to the range of programs for which we are responsible. I am proud and humbled to lead these efforts on behalf of the Treasury Department and am grateful for the opportunity to help advance our work on behalf of our national security.

**Report to Congress Pursuant to Section 243 of the Countering America's Adversaries Through Sanctions Act of 2017 Regarding Interagency Efforts in the United States to Combat Illicit Finance Relating to the Russian Federation**

**August 6, 2018**

Section 243 of the Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA) requires the Secretary of the Treasury to submit to the appropriate congressional committees not later than one year after CAATSA's enactment, and at the end of each 1-year period thereafter until 2021, a report describing interagency efforts in the United States to combat illicit finance relating to the Russian Federation. Pursuant to Section 243(e), the report shall be submitted in unclassified form, but may contain a classified annex. This document serves as the first unclassified report submitted by the Secretary under CAATSA Section 243; additional information is provided in the classified annex.

In line with the 2017 National Security Strategy of the United States, which highlights Russia's global subversion and aggression, the Administration actively employs the full range of its financial, intelligence, law enforcement, and diplomatic tools to expose, disrupt, and impose costs on those responsible for Russia's malign activities. Russian conduct includes, but is not limited to: attempts to subvert Western democracies through election interference; the continued occupation of Crimea; ongoing efforts to destabilize Ukraine; the illicit procurement of sensitive defense and intelligence technologies; malicious cyber-attacks; links to transnational organized crime (TOC); support to the murderous Assad regime in Syria; gross human rights violations and corruption; and the facilitation of sanctions evasion schemes by rogue states such as Iran and North Korea. In carrying out these malign activities, Russia relies on a highly sophisticated apparatus consisting of state and non-state agents and proxies, decades of experience carrying out influence operations around the globe, and the strategic direction of Russian president Vladimir Putin.

Russia's integration into the global economy and international financial system presents an especially unique challenge compared to other states subject to U.S. sanctions such as Iran, North Korea, and Syria. For example, a substantial portion of Russian sovereign bonds are held by external investors, including U.S. pension funds, asset managers, and banks, while Russian financial institutions have extensive global market linkages through debt, equities, and derivatives.

As this report details, this Administration's efforts against this threat are among its top priorities, resulting in an unprecedented level of financial pressure against those working on behalf of the Kremlin and in key sectors of the Russian economy targeted by U.S. sanctions.

Treasury's Russia sanctions program is among our most active. Since 2017, this Administration has sanctioned 215 Russian-related individuals and entities, 199 of which were under Treasury authorities, including 136 under Ukraine/Russia-related sanctions codified by CAATSA. These actions have blocked hundreds of millions of dollars in Russian assets in the United States and caused extensive consequences to the financial interests of affected individuals and entities.

The impact of these measures is further seen in the efforts by companies around the world to separate themselves from persons we have designated, and the efforts of designated persons to seek new (often costlier) methods to move and hide funds.

The Administration understands that any effort to embark on a more positive trajectory with Russia depends on Russia's willingness to cease viewing the world through a zero-sum lens. Russia must also realize that the United States and its allies will not waver in our determination to prevent it from undermining our democracies, economies, institutions, and the values on which these pillars of global stability – ensured by U.S. leadership – will continue to stand. As part of this Administration's efforts to disrupt and deter Russia from continued acts of subversion and destabilization, and to impose costs for its ongoing aggression, the Administration has made focused financial pressure, strategically applied, a core element of our approach. Working together with our interagency colleagues and international partners, Treasury will continue to counter the corrupt and illicit financial networks of the Russian Federation in the United States and abroad, in addition to using other levers of significant economic pressure.

**Section 243(b)(1) – Efforts to identify, investigate, map, and disrupt illicit financial flows linked to the Russian Federation if such flows affect the United States financial system or those of major allies of the United States**

Efforts to Identify, Investigate, and Map Illicit Financial Flows

Russia has spent decades developing complex and resilient networks to raise, transfer, hide, and obscure the origin and movement of the funds generated through illicit activity, including corruption, sanctions evasion and illicit arms sales, and used for its malign activity. The National Intelligence Council (NIC) leads and coordinates efforts across the intelligence community (IC) to produce analysis and support policymakers regarding Russian illicit financial activity, as well as to inform efforts to identify and disrupt these illicit financial networks. As part of these efforts, IC components have continued to identify and map a myriad of networks that support and fund the full range of malign Russian activity, including by identifying new and emerging typologies and methodologies relating to Russia's illicit financial activity.

Of particular note in this regard is the classified annex to the report required under Section 241 of CAATSA. Led by the Office of the Director of National Intelligence

(ODNI), Treasury's Office of Intelligence and Analysis (OIA) and other IC elements conducted research on political figures and oligarchs, and assessed their closeness to the regime, corrupt activities, and involvement in destabilizing activities and repression. This substantial assessment was the result of a wide-ranging effort developed over the course of several months and reflected over 2,500 hours of work.

In addition to these examples of IC efforts, Section 243(b)(6) below describes parallel efforts performed by other agencies in the service of providing leads to law enforcement.

Efforts to Disrupt Illicit Financial Flows Linked to the Russian Federation

The efforts to identify, investigate, and map the illicit financial flows linked to the Russian Federation directly inform the Administration's ongoing disruption actions. Drawing upon this information, Treasury has led the U.S. campaign to impose economic and financial costs on those actors most responsible for enabling Russia to conduct its globe-spanning malign operations.

As noted above, the Administration's efforts to target malign Russian actors are among its most active illicit finance undertakings, resulting in sanctions against 215 Russian-related individuals and entities under this Administration. Of these, Treasury's financial sanctions have been particularly powerful, imposing significant costs on targeted Russian actors and meaningfully impacting their ability to raise, move, and obscure the origin of illicit funds.

However, the impact of these sanctions and other financial measures is far greater than the amount of funds frozen. This is demonstrated by the efforts of companies around the world to distance themselves from sanctioned persons, and the efforts of designated actors to adopt new, often more difficult ways of moving and hiding their funds. From such reactions, it is clear that our measures have succeeded in imposing significant costs on those undermining U.S. interests and those of our partners and allies, in addition to disrupting such conduct. The following paragraphs illustrate numerous discrete examples of disruption efforts targeting the wide variety of Russian malign activities.

*Designations of Oligarchs and Senior Government Officials*

On April 6, 2018, Treasury sanctioned 38 individuals and entities, comprised of seven Russian oligarchs, 12 companies they own or control, 17 senior Russian government officials, and Russia's primary state-owned arms trading concern along with its bank subsidiary. Many of these individuals were appointed to their posts by Putin and hold prominent positions in the government and Russian business community. These designations delivered on Secretary of the Treasury's commitment, immediately following submission of the CAATSA Section 241 report, to impose sanctions on oligarchs and officials identified in the report.

Among those sanctioned on April 6 are oligarchs Oleg Deripaska and Viktor Vekselberg; the heads of state-owned companies such as Gazprombank, VTB Bank, and Gazprom; as well as the head of the Russian Security Council and the Russian Minister of Interior.

Among the 12 companies sanctioned are Renova Group, an international group of asset management companies and investment funds owned by Vekselberg; RUSAL, the second-largest producer of aluminum in the world; EN+, a holding company for Deripaska's metals and energy assets; Gaz Group, Russia's leading producer of commercial vehicles; and EuroSibEnergo, one of Russia's largest independent power companies.

As a result of his designation, open sources estimate that Deripaska's personal net worth has dropped by more than 50%.

The April 6 actions also had a major impact on another sanctioned oligarch, Viktor Vekselberg. According to reliable press reports, Vekselberg's net worth has dropped nearly USD 3 billion, from an estimated USD 16.4 billion on April 5, 2018 to an estimated USD 13.5 billion as of July 26, 2018. Among the 12 companies sanctioned on April 6 was Vekselberg's Renova Group, an international group of asset management companies and investment funds. As a result of the action, Renova Group was forced to divest from Swiss-based industrial company Sulzer AG, of which Renova Group was a majority shareholder. Sulzer AG bought back five million of its own shares from Renova Group following an emergency meeting days after Renova Group's designation. Renova Group was also forced to divest 20 percent from Italy-based IT company Octo Telematics, in which it had a 65 percent stake, to enable the company's continued operation and planned IPO. Moreover, U.S.-based investment management firm Columbus Nova, which manages Vekselberg's assets and counts Renova Group as its biggest client, has had to significantly limit its operations following the April 6 action.

These actions are also a part of Treasury's efforts to counter Russian sanctions evasion by "following the money" and targeting those who support designated persons in moving or concealing their assets. In designating Kirill Shamalov on April 6, for example, Treasury sanctioned an individual who received assets from Gennadiy Timchenko, who was previously sanctioned by Treasury for his support to senior Russian officials.

*Cyber Designations*

The April 6 actions were but the latest and most significant of a continuing series of designations taken in response to Russia's malign activities. By that time, in March 2018, Treasury had already exercised its authorities under Executive Order 13694 and CAATSA to take aim at entities and individuals involved in interfering in U.S. elections as well as for perpetrating damaging cyber-attacks. Part of this designation tranche targeted Russian intelligence organizations – the Federal Security Service (FSB) and the

Main Intelligence Directorate (GRU) – both of which engage in activities that undermine U.S. cybersecurity on behalf of the Russian government. Specifically, the GRU interfered in the 2016 U.S. election through cyber-enabled means while the FSB has utilized its cyber tools to maliciously target those critical of the Russian government, Russian politicians, and U.S. government officials.

This designation tranche also targeted Russian oligarch Yevgeniy Viktorovich Prigozhin, who Treasury previously sanctioned for his material support to the Russian regime. The March 2018 designation further exposed his malign conduct, as evidenced by the fact that Prigozhin also funded the operations of the Internet Research Agency, which has covertly worked on behalf of the Kremlin to influence social media networks in Russia and abroad, including the United States.

In its most recent cyber-related action, on June 11, 2018, OFAC designated an additional five Russian entities and three Russian individuals under Executive Order 13694 and CAATSA Section 224. The primary targets that were designated, Digital Security (a Russia based private cyber security firm), Kvant (a Russian state research institution), and Divetechnoservices (a Russia based private underwater technologies firm), provided technological support to the FSB and served as enablers of the organization. Treasury also took action against several entities and individuals that were owned or controlled by or acted for or behalf of these entities. These actions were taken in order to respond to Russia's continued involvement in conducting malicious cyber-attacks, restricting those who enable the FSB's destructive activities from the U.S. financial system, and to raise the costs on those who do business with the FSB.

Digital Security, for example, developed a tool for the FSB that would increase the agency's offensive and defensive cyber capabilities. As part of Treasury's action, ERPScan and Embedi, both private cybersecurity firms, were also designated for being owned or controlled by Digital Security. Russia has also been actively tracking underwater communication cables, which carry the majority of the world's communication traffic. Since 2007, Divetechnoservices has procured a variety of underwater and diving systems for Russian government agencies, to include the FSB. Specifically, in 2011 it was awarded a contract to procure a submersible craft for the FSB, valued at USD 1.5 million.

*Designations Related to Russian Activity in Crimea/Ukraine*

In January 2018, OFAC sanctioned 21 individuals and nine entities under its Russia/Ukraine authorities, as well as identified 12 subsidiaries that are owned 50% or more by previously sanctioned Russian companies to provide additional information to the private sector to assist with sanctions compliance. This action targeted major Russian companies that have played a key role in supporting Russia's attempts to integrate

Crimea into its own economy and infrastructure. ZAO VAD, for example, is a Russian company responsible for the construction of a major highway in Crimea that will serve as a primary connection between the Kerch bridge and other cities in Crimea. The projected cost for this project is nearly USD 3 billion. OFAC also sanctioned Power Machines, a large Russian engineering firm with extensive operations around the world, because of Power Machines' support to the U.S.-sanctioned company Technopromexport, one of the key companies involved in the construction of power plants in Crimea.

Also in this January 2018 action, OFAC sanctioned three individuals and four entities involved in the illicit trade of coal from the so-called Donetsk and Luhansk People's Republics, including some working with designated Yanukovych associate Sergey Kurchenko, to export coal from the separatist republics to Russia and Europe.

*Human Rights and Corruption Designations*

Implementing authorities granted under the Global Magnitsky Human Rights Accountability Act ("Global Magnitsky"), the Administration issued two Russia-related sanctions in December 2017 that highlighted significant corruption as well as human rights abuses in Russia and Ukraine. On December 21, 2017, the President imposed sanctions on persons from around the world in the Annex to E.O. 13818 implementing the Act, including Russian nationals Sergey Kusiuk and Artem Chayka. While in charge of 290 elite Ukrainian police officers, Kusiuk was a leader of an attack on peaceful protesters on November 30, 2013, many of whom took part in the beating of activists. Kusiuk has also been named as an individual who took part in the killings of activists on Kyiv's Independence Square in February 2014. Kusiuk ordered the destruction of documentation related to the events, fled Ukraine, and is now in Moscow, where he was identified dispersing protesters as part of a Russian riot police unit in June 2017.

Chayka is the son of Russia's Prosecutor General and has leveraged his father's position to unfairly win contracts and put pressure on business competitors. In 2014, Chayka's competitor for a highway reconstruction project suddenly fell under prosecutorial scrutiny and was forced to shut down, leaving Chayka in position to non-competitively work on the highway project. Also in 2014, Chayka's competitor contested Chayka's winning bid on a state-owned stone and gravel company and filed a lawsuit, after which his home was raided and he was indicted. After Chayka's competitor withdrew the lawsuit, prosecutors dropped all charges.

In December 2017, OFAC issued its sixth tranche of sanctions under the Sergei Magnitsky Rule of Law Accountability Act of 2012, bringing to 49 the total number of individuals targeted by OFAC under this authority. This round of names included Ramzan Kadyrov, the Head of the Chechen Republic, who oversees an administration involved in disappearances and extra-judicial killings. Following his designation

Kadyrov was removed from a major social media site, limiting his ability to engage in propaganda – apparently to his great consternation.

*Syria Sanctions Program*

On April 6, 2018, OFAC also designated Rosoboronexport (ROE), a state-owned corporation managing Russian weapons exports, and its banking subsidiary Russian Financial Corporation Bank (RFC). ROE has longstanding ties to the Government of Syria, with billions of dollars in weapons sales over more than a decade.

*North Korea Program*

Since the beginning of the current administration, Treasury has designated 17 targets in Russia under its North Korea authorities, including five Russian companies (including one bank), four Russian individuals, seven North Korean financial/trade/weapons representatives, and one North Korean labor firm. Most recently, on August 3, 2018, OFAC designated Russian-registered Agrosoyuz Commercial Bank for knowingly conducting or facilitating a significant transaction on behalf of the U.S. and UN-designated Moscow-based chief representative of Foreign Trade Bank (FTB), North Korea's primary foreign exchange bank. As of 2016, Agrosoyuz had opened new accounts for a North Korean front company, processed over USD 8 million and held the equivalent of over USD 3 million on behalf of the U.S. and UN-designated Korea United Development Bank. On the same day, OFAC also designated Ri Jong Won, the Moscow-based deputy representative of FTB. These designations further exposed the extent of North Korea's activities in Russia, including weapons-related acquisitions, placement of financial representatives in violation of UNSCRs, oil procurements, and overseas laborers generating revenue for the regime.

In considering the impacts of Treasury's designations, it is important to understand that what we are able to observe is but a part of the estimated effect of our actions. Business rejected, bank accounts closed, investments avoided, and funds transfers denied assuredly occur with some regularity, even if they are not made known to us. They also provide an opportunity for future diplomatic engagement or law enforcement action. The impacts of these designations go well beyond their immediately observable effects and can be built upon in the future.

In addition Treasury frequently undertakes engagement with foreign counterparts and the private sector – including intelligence and information-sharing – to disrupt the activities of malign actors. Illustrations of these efforts are described in greater depth in Section (b)(2), (b)(3), and (b)(7) below.

**Section 243(b)(2) – Efforts to conduct outreach to the private sector, including information sharing efforts to strengthen compliance efforts by entities, including financial institutions, to prevent illicit financial flows described in paragraph (1)**

Financial institutions and other businesses often stand on the front lines against illicit financial activity. Indeed, disruptive impacts like those described above depend in large part on the business community's compliance with our sanctions. Accordingly, engaging and educating the private sector to ensure that our sanctions programs are as effective as possible is a core Treasury function. In light of Russia's linkages to the U.S. and global economy, these efforts are a particular priority in our comprehensive approach to targeting Russia and Russian malign actors.

To address the incredibly high volume of inquiries from commercial and financial entities that results from this interconnectedness, Treasury has been extraordinarily active in engaging with key public and private counterparts closely to ensure the private sector as well as allies and foreign partners understand our sanctions on Russia and are able to fully implement them, as well as that they understand the broader illicit finance threats emanating from Russia.

As part of these efforts, OFAC communicates its actions to the compliance community through Recent Action Notices, which are sent to a large distribution list of over 50,000 recipients, and through Treasury press releases describing in detail the basis for Treasury designations. All sanctioned individuals and entities are placed on OFAC's List of Specially Designated Nationals and Blocked Persons or Sectoral Sanctions Identification List, which puts the regulated public on notice and which is used to populate compliance screening tools and inform global compliance programs. Although routine, these actions are critical to keeping the private sector informed of OFAC's sanctions actions.

To amplify Treasury actions, senior Treasury officials frequently engage with senior executives, including compliance officials, at foreign financial institutions and other businesses regarding our Russia program and other applicable sanctions, affirm Administration policy towards Russia, and underscore our enforcement posture towards entities that facilitate malign Russian activity. Treasury also holds roundtables with banks in jurisdictions at elevated levels of risk for Russian money laundering, including Cyprus and Latvia, to convey concerns over this issue and urge the authorities to take steps to prevent the exploitation of their respective financial sectors by bad actors.

In addition, at least once a year OFAC organizes a public symposium to discuss its sanctions programs. Most recently, in November 2017, OFAC's symposium was attended by close to 1,000 people, including legal and compliance professionals, interlocutors from foreign partners and allies, and leaders from both U.S. and

multinational businesses, some of whom helped moderate public discussions of Treasury's CAATSA guidance.

OFAC also routinely engages in outreach with the private sector by sending representatives to various trade and sanctions conferences in the United State and abroad, these representatives give speeches, presentations, and answer sanctions compliance questions. In the last year many of these conferences have devoted significant time to issues raised by CAATSA and recent sanctions actions against Russia. OFAC also engages with trade groups representing U.S. and international business interests. The detailed feedback that OFAC receives from these contacts is crucial to understanding the impact of Treasury's sanctions and tailoring current and future sanctions in ways that avoid undesirable collateral consequences.

While it has been a long-standing practice of Treasury to undertake such outreach to the private sector, we have dedicated especially significant resources to ensuring that the financial sector understands the requirements created by CAATSA. Once key provisions of CAATSA became effective, OFAC established a CAATSA landing page on its website that clearly set out all of the public guidance that OFAC and the State Department had issued. OFAC has also released a number of CAATSA-related FAQs to provide specific guidance to the public regarding the implementation of key provisions of CAATSA sections 223(a), 226, 228, and 233. These FAQs were the result of extensive U.S. government outreach to our allies and partners as well as private sector companies.

Additionally, OFAC amended and reissued Directives 1, 2, and 4 of the sectoral sanctions under E.O. 13662 as required by sections 223(b)-(d) of CAATSA. OFAC also amended Ukraine-/Russia-related General License No. 1A and reissued the general license as General License 1B, which continues to authorize certain transactions involving derivative products that would otherwise be prohibited pursuant to Directives 1, 2, or 3, and updated a number OFAC FAQs to account for the fact that CAATSA-related prohibitions in Directives 1 and 2 were now in effect. These actions communicated sanctions prohibitions and authorizations directly to the public and private sector.

OFAC's Compliance division also regularly fields calls from the private sector to explain CAATSA and provide guidance on adhering to its requirements. Since the passage of CAATSA, OFAC has responded to thousands of phone and email inquiries regarding CAATSA and Russia-related sanctions questions. OFAC Licensing provides a valuable interface for the public, where the private sector can seek a license or receive interpretive guidance related to a particular regulatory matter or fact pattern.

Large and impactful sanctions actions such as those taken against major Russian oligarchs also require extensive private sector outreach and communication. Following the April 6 designations, Treasury officials engaged in extensive discussions with allies

and partners, as well as companies linked to the sanctioned persons, to identify ways to mitigate the negative impact on global markets while simultaneously imposing costs on targeted Russian actors by compelling these firms to reduce the ownership and interest of sanctioned persons.

As the primary regulator responsible for money laundering and illicit finance activity, FinCEN also closely engages with the private sector, including to identify and disseminate information on emerging typologies supporting illicit financial actors such as Russia.

With respect to proliferation finance, the FBI Counterproliferation Center – Russia (CPC-3) has worked closely with FinCEN and a consortium of financial institutions through the FinCEN Exchange Program to enhance information sharing with the private sector. Specifically, CPC-3 has shared Russian proliferation finance typologies to initiate information sharing among banks that could lead to the uncovering of complex Russian illicit financial networks and develop actionable leads through Bank Secrecy Act reporting – including but not limited to Suspicious Activity Reports. These efforts assist CPC-3's efforts to identify illicit financial networks that aid in the procurement of U.S.-sensitive technology and allow for timely and effective law enforcement disruptions.

Further, in its posts and missions abroad, the State Department conducts regular, significant outreach to the private sector, including at conferences in the United States and abroad that focus on sanctions policy, compliance, and enforcement. These conferences are attended by sanctions practitioners, compliance professionals, and lawyers. State, often in conjunction with Treasury officials, also engages in regular meetings with private sector companies in order to explain our policies in relation to Russia, including our intent to prevent illicit financial flows.

**Section 243(b)(3) – Efforts to engage and coordinate with allied international partners on illicit finance, especially in Europe, to coordinate efforts to uncover and prosecute the networks responsible for illicit financial flows described in paragraph (1), including examples of that engagement and coordination**

Foreign Engagement with International Partners

Engagement and coordination with allies and partners are essential elements of the Administration's efforts to counter Russian malign influence. Both in Washington and in European capitals, Treasury and State engage routinely at senior and staff levels to share information about, coordinate approaches to, and forge common understandings of this shared threat.

Since the passage of CAATSA, Treasury and the State Department have traveled extensively through Europe – including the United Kingdom, Germany, France,

European Union, Italy, Poland, Denmark, the Netherlands, Lithuania, Estonia, Latvia, and Finland – to discuss the implementation of the Russia-related provisions of that statute with foreign and finance ministries. Treasury and the State Department have also engaged with international partners through the G-7+ Contact Group (United States, United Kingdom, Germany, France, Italy, Canada, Australia, European Union, Norway, and Poland), a group of likeminded countries coordinating efforts to counter Russian malign influence and continue exerting pressure on the Kremlin to implement the Minsk agreements. The Department of Homeland Security has engaged European partners through the G7 Security Ministers and U.S.-EU Justice and Home Affairs Ministerial meetings to coordinate similar efforts to counter Russian malign influence. Treasury and State also actively engage with the European External Action Service (EEAS) of the European Union, which has provided useful feedback and insight on the impact of CAATSA and the recent April 6 action on the European economy.

These engagements also provide important opportunities for the Administration to press European partners to develop and employ the necessary tools to effectively counter common threats such as Russia, including domestic sanctions authorities where they do not exist, and to enhance the ability of their financial intelligence units to collect, analyze, and share information, including with respect to illicit Russian financial activity. Senior Treasury officials have also regularly emphasized the Administration's strong opposition to Nord Stream II, which if completed would generate additional funds the Kremlin could use to finance its malign activity, while simultaneously deny Ukraine substantial transit revenues it needs to defend itself against Russian aggression.

The Administration has prioritized engagement with jurisdictions with high volumes of Russian financial flows, including the United Kingdom, Cyprus, and Latvia, to advance U.S. objectives on Russia. As elaborated below, such engagement and coordination significantly expands the reach and impact of our unilateral efforts to disrupt illicit Russian financial activity, amplifies multilateral messaging that the U.S. and its partners will not tolerate Russian aggression, and helps maintain transatlantic unity against a Russia bent on undermining these historic ties.

United Kingdom

The scale of the UK financial services market and access to the EU have made London and UK overseas territories such as the British Virgin Islands an attractive destination for illicit financial flows.The UK National Crime Agency has estimated that, "many hundreds of billions of pounds of international criminal money is laundered through UK based banks and subsidiaries each year," to include Russian oligarch proceeds of corruption. Recognizing this, the United States and UK have regularized consultation and cooperation to coordinate our respective efforts to counter Russian malign influence, including its financial activity.

Cyprus

Senior officials from State and Treasury have engaged Cypriot authorities extensively over the past year and a half to underscore concerns that Cyprus continues to host a large volume of suspicious Russian funds and investments, and have pressed Cypriot officials to harden its financial system against these threats. Vulnerabilities Cyprus presents include its permissive citizenship by investment program, its weak supervision of Administrative Service Providers, and lax company formation requirements, which are exploited by illicit actors to set up front companies and to use these fronts to open bank accounts and access the international financial system.

Although Cyprus remains a jurisdiction of concern from the perspective of Russian money laundering, the Administration is seeing some signs of progress. Following the April 6 oligarch designations, Oleg Deripaska and Victor Vekselberg both had bank accounts frozen. In May 2018 Cyprus issued a circular instructing its banks to address certain illicit finance risks from shell companies, in particular the challenges in verifying customers' background.

Latvia

Latvia has long served as a permissive environment for illicit Russian financial activity due to its geography, demography, linguistic profile, developed banking system, and membership in the European Union and Eurozone. For decades, Russian malign actors and their agents have exploited lax controls in Latvia's financial sector to launder illicit funds and support Russia's destabilizing conduct.

Under this Administration Treasury has redoubled its efforts to work with Latvia to strengthen its financial system by improving the legislative and regulatory framework as well as institutional capacity. In February 2018, pursuant to Section 311 of the USA PATRIOT Act, FinCEN issued a notice of proposed rule-making against ABLV Bank, a Latvian bank it found had facilitated significant Russian-based illicit activity. FinCEN identified ABLV Bank as a foreign financial institution of primary money laundering concern and proposed a special measure that would prohibit U.S. financial institutions from opening or maintaining a correspondent account in the U.S. on behalf of the bank. (This action is discussed in greater detail in this report under Section 243(b)(5)).

This bank's involvement in illicit financial activity reflects broader systemic deficiencies in Latvia that this Administration is working hard to address. These deficiencies reflect a historically ambivalent commitment to definitively reducing the risks Latvia faces from its high volume of non-resident deposits, many of which emanate from Russia and other Commonwealth of Independent States (CIS) countries and are held by opaque shell companies.

To strengthen the authorities in Latvia committed to redressing these vulnerabilities, senior Treasury leadership has undertaken regular, high level engagement. Working closely with Embassy Riga, senior Treasury officials have urged Latvian leadership to support and empower emerging voices in Latvia's financial sector to urge meaningful reforms, such as reducing Latvia's stock of non-resident deposits, bolstering the resources allocated to Latvia's Financial Intelligence Unit (FIU), and taking tougher enforcement action against banks that violate Latvian regulations against money laundering and sanctions evasion.

Latvia has passed legislation banning shell companies and appointed a new FIU director. Latvia has also amended its Law on Sanctions to close legal loopholes and allow the banking regulator to issue regulations to prevent sanctions evasion (See additional detail in Section (b)(4) below).

*Foreign Deployed Subject Matter Experts*

Administration departments and agencies have also forward deployed illicit finance subject matter experts to partner countries to increase international cooperation targeting Russian illicit financial flows. The BEOU program manages Assistant Legal Attaché (ALAT) positions who currently operate with two organized crime task forces in Eastern Europe. These ALATs are fully embedded members within these task forces and serve as a point of contact between the foreign partner agency and the FBI writ large.

In 2018, Treasury and the Department of Defense partnered to establish a new Treasury Liaison Officer position at U.S. European Command (EUCOM) in Stuttgart, Germany. This new Treasury liaison role will facilitate existing and establish new finance-related cooperation and information sharing among the Department of Defense, Treasury, and NATO allies.

**Section 243(b)(4) – Efforts to identify foreign sanctions evaders and loopholes within the sanctions regimes of foreign partners of the United States**

As described in greater detail under the response to Section 243(b)(1), the IC has constantly sought to identify and map out illicit financial networks supporting the Russian Federation, which includes identifying activity designed to evade existing sanctions programs.

Through its leadership in the Financial Action Task Force (FATF) – where the United States currently holds the presidency – and in FATF-Style Regional Bodies (FSRBs), Treasury also works to strengthen international anti-money laundering/countering the financing of terrorism (AML/CFT) standards and ensure that these measures are effectively implemented around the world. For example, the FATF's efforts to ensure that all jurisdictions apply a high level of scrutiny to the financial activities of politically

exposed persons (PEPs) and collect information on the beneficial owners of legal entities helps to enable the detection of detect attempts by Russian officials to launder, hide, or move the proceeds of corruption. Similarly, the FATF's work to promote the global implementation of UN sanctions and hold underperforming countries accountable through its "grey list" process helps undermine Russian attempts to circumvent international prohibitions on dealings with North Korea, Iran, or other UN-listed programs. Indeed, one of the priorities of the current U.S. presidency is proliferation finance, an effort intended to harden the world's financial systems against the type of illicit procurement and proliferation activity in which Russian actors are regularly involved.

**Section 243(b)(5) – Efforts to expand the number of real estate geographic targeting orders or other regulatory actions, as appropriate, to degrade illicit financial activity relating to the Russian Federation in relation to the financial system of the United States**

As the Administration works aggressively to deter and prevent illicit Russian financial activity abroad, it is also focused intently on protecting the U.S. financial system. Of particular recent note, as referenced above, was FinCEN's February 16, 2018 finding pursuant to Section 311 of the USA PATRIOT Act that Latvia-based ABLV Bank AS ("ABLV") was a financial institution of primary money laundering concern. In its public notice of proposed rulemaking, FinCEN cited multiple instances of institutionalized money laundering in which ABLV management solicited high-risk shell company activity that enabled the bank and its customers to launder funds. ABLV's facilitation of shell company activity typically benefitted illicit actors engaged in an array of illicit conduct, including transnational organized criminal activity, corruption, and sanctions evasion, emanating mostly from Russia and former CIS countries. Pursuant to this finding, FinCEN proposed the imposition of a prohibition on U.S. financial institutions from opening or maintaining correspondent accounts for, or on behalf of, ABLV.

FinCEN has also utilized its authorities under the Bank Secrecy Act to issue Geographic Targeting Orders (GTO) to impose additional recordkeeping requirements on domestic financial institutions or other businesses in a specific geographic area. Specifically, FinCEN has issued GTOs to collect additional financial information on transactions in the real estate sector in several jurisdictions known for attracting large amounts of foreign investors, including those from Russia.

**Section 243(b)(6) – Efforts to provide support to counter those involved in illicit finance relating to the Russian Federation across all appropriate law enforcement, intelligence, regulatory, and financial authorities of the Federal Government, including by imposing sanctions with respect to or prosecuting those involved**

Treasury's Office of Intelligence and Analysis, FinCEN, CIA, and NSA, among other agencies, play critical roles in the Administration's work to support law enforcement and other authorities, especially in the imposition of sanctions and other impactful measures against illicit Russian financial activity.

FinCEN conducts research and analysis of information gathered pursuant to the Bank Secrecy Act relating to Russian illicit financial activity, both domestically and overseas. FinCEN's financial intelligence products are disseminated primarily within the U.S. government, including to policymakers, law enforcement agencies, and the Intelligence Community. FinCEN also exchanges information with its counterpart financial intelligence units in other jurisdictions, including on matters related to Russian illicit finance. Additional details are provided in Section (b)(7) below.

**Section 243(b)(7) – Efforts to investigate or otherwise develop major cases, including a description of those cases**

The Administration has moved aggressively using the range of its law enforcement and regulatory tools against Russian malign activity. Descriptions of select cases are described below.[1]

The investigation of the Department of Justice's Special Counsel thus far has led to the indictment of 25 individuals and three companies for a variety of offenses – including conspiracy to commit wire fraud and bank fraud and conspiracy to launder money – committed in furtherance of Russia's scheme. The indictments describe a variety of methods used by the defendants to fund their operations.

As alleged in an indictment filed in February 2018, one element of the operation involved the use of two related companies to channel millions of dollars' worth of funds to approximately fourteen affiliated companies that in turn provided money to an organization that sought to engage in "information warfare against the United States" and to "spread distrust towards the candidates and the political system in general." Certain of the defendants in this part of the operation also used stolen personal information to open accounts at a digital payment service provider.

In another element of this influence operation focused on hacking into the United States, as described in the Special Counsel's July 2018 indictment, 11 Russian individuals affiliated with Russia's military intelligence agency, the Main Intelligence Directorate of the General Staff (GRU), conspired to launder the equivalent of more than $95,000 using cryptocurrencies such as bitcoin to lease servers, register domains, purchase at least one

[1] As with the classified version of this report, this unclassified version of the report does not discuss in detail open or pending investigations, law enforcement investigations or activities, or other disruptive actions ongoing at the time of release that have not been publicly disclosed in charging documents.

virtual private network account, and make other payments in furtherance of their hacking activity. As the indictment highlights, the conspirators engaged in a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin in their financial transactions with U.S. payment processing companies, including to pay web hosting companies, domain registrars and other businesses. The conspirators also allegedly mined bitcoin, purchased bitcoin through peer-to-peer exchanges, moved funds through other digital currencies, used pre-paid cards, and worked with a third-party exchanger that enabled layered transactions through digital currency platforms.

In July 2017, FinCEN assessed a $110 million dollar penalty against virtual currency exchange BTC-e (operated by a Russian citizen) for its failure to implement even basic controls to prevent the use of its services for illicit purposes. BTC-e's lack of effective supervision led to it being exploited by a customer base that included many criminals who desired to conceal proceeds from crimes such as ransomware, fraud, identity theft, public corruption, and drug trafficking. BTC-e permitted and failed to report millions in transactions from ransomware such as Cryptolocker and Locky. Importantly, FinCEN's BSA enforcement investigation also led to the assessment of a $12 million civil money penalty against one of BTC-e's administrators, Alexander Vinnik – the largest individual liability penalty FinCEN has assessed to date. At one point BTC-e served approximately 700,000 customers across the world and was associated with bitcoin wallets that had received over 9.4 million bitcoins. It also offered exchange in fiat currency, as well as convertible virtual currencies Bitcoin, Dash, Litecoin, Namecoin, Novacoin, Peercoin, and Ether. In conjunction with FinCEN's enforcement action, Alexander Vinnik and BTC-e were also indicted by the Department of Justice for operating an unlicensed money service business, money laundering, and related crimes.

FBI is also partnering with FinCEN to detect and disrupt illicit financial flows linked to the Russian Federation. Drawing on primarily wire transfer datasets shared by FinCEN and a dataset derived from the Panama Papers leak revealed by the International Consortium of Investigative Journalists, FBI used analytic platforms to assist in processing nearly 4,000,000 international wire transfers centered on four Balkan and Cypriot banks known by FinCEN to facilitate illicit Russian financial flows. This effort enabled the FBI to expand its understanding against Russian-linked offshore financial networks, identified a variety of new FBI targets, and enhanced FBI understanding of existing investigations. Impacts under this initiative include but are not limited to the following:

- FBI opening of a sensitive internal joint investigation by a counterintelligence and public corruption squad against a high level state elected official.

- A targeting and potential intelligence reporting platform using links between FBI-derived information and Russia-affiliated entities in FinCEN-FBI data holdings, including several TOC and various criminal targets.

FBI also has an open investigation on a multi-billion dollar international money laundering operation also tied to U.S. locations, owned and operated by an identified Eurasian billionaire with strong ties to Eurasian organized crime. FBI developed U.S. law enforcement, U.S. intelligence, and international law enforcement partners to enhance this investigation.

**Conclusion**

As evidenced by the comprehensive efforts illustrated above, the Administration is aggressively targeting and disrupting the illicit financial networks supporting Russian malign activity. The Department of the Treasury, in close coordination with other departments and agencies, will continue to impose costs upon those acting on behalf of the Kremlin against U.S. interests and increase financial pressure on Russia to advance our national security priorities. Additional information on the full range of the Administration's efforts can be found in the classified annex to this report.

## PREPARED STATEMENT OF CHRISTOPHER KREBS

UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE,
DEPARTMENT OF HOMELAND SECURITY

AUGUST 21, 2018

Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for today's opportunity to testify regarding cyberthreats to critical infrastructure. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyberspace, a core homeland security mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber- and physical-infrastructure.

DHS is responsible for assisting Federal agencies in protecting civilian Federal Government networks and collaborating with other Federal agencies, as well as State, local, tribal, and territorial governments, and the private sector to defend against cyberthreats. Our work enhances cyberthreat information-sharing across the globe to stop cyberincidents before they start and help businesses and Government agencies to protect their cybersystems and quickly recover should such an attack occur. By bringing together all levels of Government, the private sector, international partners, and the public, DHS is taking action to protect against cybersecurity risks, improve our whole-of-Government incident response capabilities, enhance information sharing of best practices and cyberthreats, and to strengthen resilience.

**Threats**

Cybersecurity threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Regarding cyberthreats to our critical infrastructure, the Director of National Intelligence recently said that "the warning lights are blinking red." We have seen advanced persistent threat actors, including cybercriminals Nation-States and proxies, increase the frequency and sophistication of malicious cyberactivity. Our adversaries have been developing and using advanced cybersecurity capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy.

Although the intelligence community has not yet seen evidence that Russia intends to conduct a robust campaign aimed at tampering with our election infrastructure or influencing the makeup of the House or Senate in 2018, Russia has previously demonstrated the capability and intent to interfere with our elections. Russian efforts to influence the 2016 elections were one of the most recent expressions of Moscow's longstanding desire to undermine the U.S.-led liberal democratic order. The Russian Government conducted malicious cyberoperations by compromising and leaking emails from U.S. political figures and institutions, and targeting election infrastructure. These activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. Accordingly, we view the 2018 midterm elections as a potential target for Russian cyberoperations and are working aggressively to mitigate any foreign threats to our election systems or infrastructure.

Global cyberincidents, such as the "WannaCry" ransomware incident attributed to North Korea and the "NotPetya" malware incident attributed to the Russian military in May and June 2017, respectively, are examples of malicious actors leveraging cyberspace to create disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe. Prior to these events, DHS had already taken actions to help protect networks from similar types of attacks. NPPD's National Cybersecurity and Communications Integration Center (NCCIC) publishes a list of known software vulnerabilities and pushes this information out to stakeholders on a routine basis. Additionally, through requested vulnerability scanning, we helped stakeholders identify vulnerabilities on their networks so they could be patched before incidents and attacks occur. Recognizing that not all users are able to install patches immediately, we shared additional mitigation guidance to assist network defenders. As the incidents unfolded, we led the Federal Government's incident response efforts, working with our interagency partners, in providing situational awareness, information sharing, malware analysis, and technical assistance to affected Government and critical infrastructure entities.

In a series of incidents since at least May of last year, working with U.S. and international partners, DHS and FBI have identified Russian Government actors targeting Government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. DHS assesses that this campaign ultimately collected information pertaining to industrial control systems with the intent to gain access to industrial control systems environments. The intrusions have been

comprised of two distinct categories of victims: (1) staging and (2) intended targets. Through the Department's incident response actions, we identified activities by Russian Government actors to target certain entities that then become pivot points, leveraging existing relationships between the initial victim and the intended targets to hide their activity, as part of a multistage intrusion campaign to gain access to networks of major, high-value assets that operate components of our Nation's critical infrastructure. Based on our analysis and observed indicators of compromise, DHS has confidence that this campaign is still ongoing, and threat actors are actively pursuing their ultimate long-term campaign objectives. DHS and FBI continue to conduct incident response related to this activity and have published a joint technical alert and hosted public webinars to enable network defenders to identify and take action to reduce exposure to this malicious activity.

Since 2015, the U.S. Government received information from multiple sources—including public and private sector cybersecurity research organizations and allies—that cyberactors are exploiting large numbers of network infrastructure devices (e.g., routers, switches, firewall, Network-based Intrusion Detection System devices) worldwide. Earlier this year, DHS, FBI, and the United Kingdom's National Cyber Security Centre published a publicly available joint technical alert attributing this activity to Russian State-sponsored actors. Targets are primarily Government and private-sector organizations, critical infrastructure providers, and Internet service providers supporting these sectors. Several days after publication of the alert, an industry partner notified DHS and FBI of related malicious cyberactivity in which the actors redirected certain queries to their own infrastructure and obtained sensitive information, which included the configuration files of networked devices. Russian State-sponsored actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

**Cybersecurity Priorities**

DHS, our Government partners, and the private sector are committed to a more strategic and unified approach as we work to improve our Nation's overall defensive posture against this malicious cyberactivity. Presidential Policy Directive-21, Critical Infrastructure Security and Resilience, recognized that only a more integrated approach to managing risk would enable the Nation to counter malicious cyberactivity our adversaries. In May of this year, DHS published a Department-wide Cybersecurity Strategy, providing DHS with a strategic framework to execute our cybersecurity responsibilities during the next 5 years.

This Administration has leaned forward even further, prioritizing the protection and defense of our people and economy from the range of threats that exist today, including those emanating from cyberspace. Last year, the President signed Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. This Executive Order set in motion a series of assessments and deliverables to enable the improvement of our defenses and lower our risk to cyberthreats.

Executive Order 13800 requires continued examination of how the Federal Government and industry work together to protect our Nation's critical infrastructure, prioritizing deeper, more collaborative public–private partnerships in threat assessment, detection, protection, and mitigation. In collaboration with civilian, defense, and intelligence agencies, we have worked to identify authorities and capabilities that agencies could employ, soliciting input from the private sector, and developed recommendations to support the cybersecurity efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts. It is only through this collective defense model that we will be successful against this threat.

NPPD's NCCIC operates at the intersection of the private sector, State and local governments, Federal departments and agencies, international partners, law enforcement, intelligence, and defense communities. The Cybersecurity Information Sharing Act of 2015 established DHS as the Federal Government's central hub for the automated sharing of cyberthreat indicators and defensive measures. The NCCIC's automated indicator sharing (AIS) capability allows the Federal Government and the private sector network defenders to share technical information at machine speed,. The NCCIC also provides entities with information, technical assistance and guidance they can use to secure their networks, systems, assets, information, and maintains confidentiality with our data, by reducing vulnerabilities, ensuring resilience to cyberincidents, and private partners supporting their holistic risk management priorities. DHS does this in a way that protects privacy and civil liberties.

**National Risk Management**

We are facing an urgent, evolving crisis in cyberspace. Our adversaries' capabilities online are outpacing our stovepiped defenses. Working together with the private sector and our Government partners, we are addressing this problem and taking collective action against malicious cyberactors.

Specifically, there is a need to enhance and promote the Department's cross-sector, cross-Government coordination on critical infrastructure security and resilience.

We must improve our focus on examining the critical functions that drive our economy and facilitate national security. In other words, we need to continually advance our ability to organize and collaborate on risk strategies, planning, and solutions. For many years, DHS has worked closely with the private sector, but it has become clear that it must be a focal point for turning threat intelligence into joint action.

At the Department's first National Cybersecurity Summit this summer, in response to a clear demand signal and after extensive consultation with industry and Government partners, Secretary Nielsen announced the rebranding of the Office of Cyber and Infrastructure Analysis (OCIA) as the National Risk Management Center (NRMC). Housed within DHS, the NRMC is the logical evolution of the ongoing improvements made over the last several years in information sharing and partnership building between the Government and industry. The NRMC draws on existing resources and functions from across NPPD, the Department and our Federal and international partners to bring our risk management efforts to the next level in effectiveness.

The NRMC's mission is to continually facilitate analysts and planners, from both public and private sector, in their efforts to assess our country's cyber-risks, plan to combat those risks and—most importantly—enable implementation of tailored solutions to protect our networks. The full expertise of the Federal Government should be brought to bear on these challenges. With this in mind, the NRMC will provide the private sector with an entrance point for project teams to access programs from all departments and agencies and coordinate defenses against cyberthreats that can affect all sectors.

Perhaps most importantly, the Center's core mission focuses on the systems or functions that cut across sectors. Ultimately, the Center will facilitate a partnership among and across Government and industry that can provide a unified, collective approach to the defense that the Nation needs to achieve superiority over our adversaries.

We cannot fail to evolve as the threats continue to come. The NCCIC and National Infrastructure Coordination Center (NICC) will continue to carryout current operations but the NRMC will enhance their efforts. The NRMC will support NCCIC and NICC operations by helping with prioritization and other needs, while also looking ahead to plan more strategically, and leveraging feedback from the operations and other partners.

**Election Security**

DHS is committed to ensuring a coordinated Federal Government effort to assess vulnerabilities and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. Based on our assessment of activity observed in the 2016 elections, DHS and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our allies.

Under the Constitution and our system of laws, State and local election officials in thousands of jurisdictions administer Federal elections. Risk management for election officials did not begin in 2016. State and local election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of U.S. elections. DHS is working with all 50 States to provide value-added—yet voluntary—services to support their efforts to secure elections.

This year our Nation is in the midst of primary and special elections as well as the general election in November. We have been working with election officials in all States to enhance the security of their elections by offering support and by establishing essential lines of communications at all levels—public and private—for reporting both suspicious cyberactivity and incidents. This information sharing is critical and our goal is to enhance transparency and have visibility of aggregated elections-related cybersecurity efforts. We are also working with election officials, vendors, the Election Assistance Commission (EAC), and National Institute of Standards and Technology (NIST) to characterize risk to election systems and ensure appropriate mitigations are understood and available in the marketplace. As a part

of this process, we work with these stakeholders to recommend best practices to ensure a secure and verifiable vote. Through the Government Coordinating Council, we also developed guidance for States on how best to spend funding received through the Help America Vote Act grant issued by the EAC.

DHS has made tremendous progress and has been committed to working collaboratively with those on the front lines of administering our elections—State and local election officials and the vendor community—to secure election infrastructure from risks. Engagement with all 50 States and the establishment of the Election Infrastructure–Information Sharing and Analysis Center with nearly 1,000 members reflects the advances we have made in building a coalition committed to securing elections from cyberthreats. The establishment of Government and sector coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyberinfrastructure. However, we recognize that there is a significant technology deficit across State and local governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that systems are upgraded and insecure or vulnerable systems are retired.

**Conclusion**

In the face of increasingly sophisticated threats, DHS employees stand on the frontlines of the Federal Government's efforts to defend our Nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyberthreats. Our infrastructure environment today is complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient while not endangering freedom of speech, freedom of religion or failing to protect an individual's privacy. Technological advances have introduced the "Internet of Things" and cloud computing, offering increased access and streamlined efficiencies, while increasing access points that could be leveraged by adversaries to gain unauthorized access to networks. As new threats emerge, we must better integrate cyber and physical risk management in order to secure effectively the Nation. Expertise in cyberphysical risk assessments and cross-sector critical infrastructure interdependency evaluation is where NPPD brings unique experience and capabilities.

We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future, and we appreciate this Committee's leadership in working to establish the Cybersecurity and Infrastructure Security Agency to accomplish this goal. We are committed to working with Congress to ensure that we address cybersecurity in a way that cultivates a safer, more secure and resilient Homeland.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

---

**PREPARED STATEMENT OF CHRISTOPHER A. FORD**

ASSISTANT SECRETARY, BUREAU OF INTERNATIONAL SECURITY AND NONPROLIFERATION, DEPARTMENT OF STATE

AUGUST 21, 2018

Chairman Crapo, Ranking Member Brown, and Senators, thank you for inviting us.

I represent the Bureau of International Security and Nonproliferation (ISN), and I am pleased to join Treasury Under Secretary Sigal Mandelkar and DHS Under Secretary Christopher Krebs, to help explain how we are employing the various sanctions tools Congress has given us vis-a-vis the Russian Federation and the various malign activities of the Putin regime. For my part, I will be focusing principally upon Section 231 of the Countering America's Adversaries Through Sanctions Act of 2017 (or CAATSA), because implementation of that section has been entrusted to my bureau at the State Department.

But if I might, Mr. Chairman, before I talk about our approach to implementing Section 231, I'd like first to put my bureau's work in this respect into a broader context.

**Our Philosophy of CAATSA Section 231 Implementation**

At the ISN Bureau, our traditional focus is upon the myriad threats and policy challenges facing the United States from the spread of weapons of mass destruction (WMD), to delivery systems, and advanced conventional weapons. These issues are of enormous importance to national and international security, of course, and ISN's

eponymous role in "international security" has been seen primarily through the nonproliferation prism.

But "international security" can—and does—encompass more than just nonproliferation, and one of our roles is to implement sanctions under Section 231 of CAATSA. In passing that legislation last year, Congress made very clear its intention that the purpose of the Russia sanctions provisions therein was to pressure Russia to change its behavior with respect to a wide variety of malign acts—including Vladimir Putin's effort to interfere in the 2016 U.S. presidential election. We have heard that message loud and clear.

Significantly, there is more to this than a much-deserved response to malign acts and deterrence to such provocations in the future—though those are, of course, laudable goals that we fully support, and which we are using CAATSA to help bring about. As I see it, these sanctions tools also have value in better equipping us to play a role in broader arenas of great-power competition and geopolitical competitive strategy.

The new National Security Strategy calls out "the contest for power" as "[a] central continuity in history," and warns about challengers—specifically, "the revisionist powers of China and Russia, the rogue States of Iran and North Korea, and transnational threat organizations"—that "are actively competing against the United States and our allies and partners."

Similarly, the new National Defense Strategy observes that "[t]he central challenge to U.S. prosperity and security" today is "the reemergence of long-term, strategic competition." "It is increasingly clear," that document states, "that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other Nations' economic, diplomatic, and security decisions." Indeed, the NDS notes that "[b]oth revisionist powers and rogue regimes are competing [with the United States] across all dimensions of power."

This is the mindset that we also bring to approaching CAATSA sanctions against Russia. Russia has undertaken a campaign of malign activities in its attempt to compete with the United States and our allies and partners. The array of sanctions the United States has imposed against Russia, and those that materially support its malign activities, respond directly to its aggressive action against our country, our allies, and our partners.

And this is where CAATSA's Section 231 comes into play. The threat of mandatory sanctions against individuals or entities that have engaged in significant transactions with the Russian defense or intelligence sectors can be so useful, but we need to use this powerful tool surgically—to excise the malignancy without damaging our very important foreign relationships. As we have been implementing Section 231, we began by emphasizing to our allies that transactions with the Russian arms industry could have consequences.

Firstly, these are the same arms that Russia used and continues to use in its aggression against Ukraine. Our implementation of the CAATSA sanctions reinforces this Administration's unwavering commitment to Ukraine's sovereignty and territorial integrity, including over Crimea.

Secondly—as Willie Sutton reportedly said when asked why he robbed banks—"that's where the money is." High-technology military equipment is one of the only competitive sectors of the Russian economy these days, and Moscow makes a great deal of money from selling arms abroad indiscriminately—be it to Iran or the Assad regime. These funds fuel the Kremlin's malign activities, spread its malign influence, and support Russia's development of newer, even more deadly weapons. Accordingly, if Russia is to feel pressure in response to its malign activities, it makes sense to go after these revenues—revenues that may also help offset the costs of developing newer, even more deadly weapons that threaten and undermine the security of the United States and our allies and partners.

More broadly, however, Russia also uses its arms transactions as a tool of geopolitical influence. For Russia, it isn't just about money, but about the relationships that the arms trade creates for Moscow. Scaling back and shutting down Russia's arms deals and deterring such transactions in the future strike directly at the Kremlin's malign activities and influence that it seeks to exert in the international community.

That is our central philosophy behind Section 231 implementation. The broadest challenge, of course, is how to manage a relationship with Russia that has both important cooperative aspects and important points of disagreement. As the President and Secretary Pompeo have made clear, we seek to cooperate with Russia on subjects of shared interest wherever we can, because of course there are important shared interests on which it would be irresponsible of us not to cooperate. This was, for instance, well symbolized by the conference we held at the State Department on June 28 that brought together the United States, United Kingdom, and the Russian

Federation as the Depository States of the Nuclear Nonproliferation Treaty (NPT), to commemorate the 50th Anniversary of that Treaty being opened for signature. For the occasion, the three foreign ministers of these Depository States issued a joint communique reaffirming their shared commitment to the NPT and the nonproliferation regime of which it is the cornerstone.

At the same time, the Department and my Bureau have not been shy about acting forthrightly in pushing back against Russian malign activities. The sanctions tools you have given the State Department, including CAATSA's Section 231, are valuable elements of how this Administration is contributing to American success in responding to Russian aggression in this new era of great power competition.

**A Record of Successes to Date**

As we have dispatched our diplomats repeatedly around the world to spread word about Section 231 and encourage Russia's arms clients to wean themselves from Moscow, we have had some notable successes to date. Most of these successes are ones about which it is not possible or advisable to speak in public, because most interlocutors who take action to reduce their exposure to Section 231 sanctions are not keen to publicize the fact. We very much wish to respect their sensibilities, because that's how friends treat each other. We also want to honor these confidentialities because embarrassing partners who have done the right thing in reducing their Russian arms entanglements isn't a good way to encourage others to follow suit—we are also cognizant of potential Russian retaliation against these interlocutors.

Nevertheless, though we can't speak about them publicly, we have had real successes—in the form of something on the order of billions of dollars in announced or expected Russian arms transactions that have quietly been abandoned as a result of our diplomatic outreach about Section 231. That's billions that Putin's war machine will not get, and through which the Kremlin's malign influence will not spread, and a slew of strategic relationships between the Kremlin and overseas partners that will not broaden and deepen. We're proud of this record, and we're working hard to run up the score further.

So effective has the threat of CAATSA sanctions been to date, moreover, that we have been able to do all this without imposing sanctions on a friend or partner State of our own. I urge you not to look at the scorecard as whether the United States has imposed sanctions. In this case, sanctions reflect our failure to turn off Russian arms deals. The time will come when we will have no choice but to impose sanctions, but we are keenly aware that Congress' purpose in passing Section 231 was to pressure Russia and incentivize Russia to change its behavior, not to hurt U.S. friends and allies who might happen to purchase arms from Moscow.

**Six Principles for Implementation**

Mr. Chairman, I will be happy to answer any questions you have about these matters—at least as best I can in an open forum. I am also very happy to participate in or send briefers for a closed session. Before I conclude, however, let me say a few more words about our approach to Section 231. In particular, I'd like to outline six principles that help guide our work:

1. First, as I said earlier, the target of Section 231 sanctions is Russia, not the countries that happen to purchase arms from Russia. Our interlocutors and partners need to know that although CAATSA may compel us to have challenging conversations with them, the underlying problem is not with them. Rather, our problem lies with Moscow and its own destabilizing role in the international community. I am sure that this is not always a great consolation, but it is vital that our interlocutors understand it all the same.
2. Second, we are not usually concerned with Russia's mere provision of spare parts or its maintenance of military equipment that another country already possesses. We know that many States still possess some Russian arms, and we are certainly not in the business of trying to insist that such countries give up on defending themselves. For CAATSA purposes, we are comfortable with the maintenance of equipment or the provision of spare parts not generally being considered a transaction that is considered significant under Section 231.
   Our concerns begin where and when something more consequential occurs—something such as a major transfer of foreign funds to the Russian defense sector, for instance, or a new shipment of equipment representing a qualitative upgrade in capability, such as an S-400. In such cases, the issue of "significance" becomes more problematic, and the risk of mandatory sanctions thus increases. This is the message we have been relaying to interlocutors in our diplomatic outreach, and it is one of which we hope Congress will approve.
3. Third, we have also been sending the message that a transaction generally won't be considered significant unless and until a major change in the status

quo actually occurs. Just talking about or announcing a Russian arms deal, in other words, is not generally in itself a trigger for Section 231 sanctions. The problem arises when new Russian equipment starts to show up or perhaps when large sums of money begin to change hands.

We don't expect Russia's arms clients to disavow or renounce their deals. In truth, Russia is not a very good or reliable arms partner on a good day, and even with global suppliers more reputable and reliable than Russia, consummation of a purchase of sophisticated equipment can take a long time and experience detours, obstacles, or reasons to fall apart. If in this new CAATSA environment, Russia's major arms clients never quite finalize their purchase, then the State Department will have nothing about which to have to assess "significance" under Section 231 in the first place.

4. And speaking of off-ramping, another piece of our diplomatic message has been that even with respect to new equipment, we are not necessarily asking countries immediately to go "cold turkey" on Russian arms. We understand that can be very difficult. As long as new deliveries of more advanced equipment don't occur, we have room for some flexibility vis-a-vis new purchases, provided that the overall trend line is demonstrably "down." That is, that such countries are weaning themselves off of the arms transactions that help fund Moscow's adventurism and that create geopolitical partnerships that the Kremlin can thereafter exploit for destabilizing ends.
5. With respect to the new CAATSA waiver language in the NDAA, we are glad to have greater flexibility on these issues. At Secretary Pompeo's hearing before this Committee on July 25, Chairman Corker and Senator Cardin emphasized to him that Congress views the new waiver language as narrow—in your words, Mr. Chairman, "to allow countries that we're dealing with that we wish to buy American military equipment to be weaned off Russian equipment." Secretary Pompeo, in turn, made clear his agreement—noting that the new waiver is a way to avoid driving countries with historical Russian entanglements more into Moscow's arms while permitting them "the capacity of spare parts" or to "round out th[e] process" of weaning themselves of their dependency on Russia. We will use this understanding to guide implementation of Section 231.
6. Finally, it's worth pointing out that Section 231 only applies to Russian arms transactions. To the extent that a country contemplating a purchase of advanced Russian equipment can pursue alternative sources of supply in meeting its defense needs, therefore, this is an excellent way to avoid sanctions liability. Purchases from European or other international suppliers of sophisticated weaponry, for instance, would raise no Section 231 concern. Nor, of course, would purchases from the United States—and we are always happy to try to facilitate discussions with relevant U.S. interlocutors about such possibilities.

These principles help guide our Section 231 diplomacy, and I think they are producing some very good results for the United States.

Mr. Chairman, I am pleased to have had the chance to explain our approach to Section 231 of CAATSA, and I look forward to taking your questions. Thank you.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM SIGAL P. MANDELKER**

**Q.1.** *CAATSA Implementation:* Many of us on both sides have repeatedly urged more assertive implementation of mandatory sanctions under CAATSA, in order to deter further Russian attacks. I know you have begun to do a bit more in recent months, and in some cases would prefer to use EO authorities because you see them as more flexible. But there is still a lot more that could be done with mandatory CAATSA sanctions.

Can you give us a more precise sense of what you have planned before the elections to signal more powerfully to Russia's leaders that they must stop—and what you are preparing for generally, in terms of escalation, if the Russians continue their aggressive actions through the elections and beyond?

What are the general sanctions areas—banking, energy, sovereign debt, sectoral sanctions, or a mix of all of them—that you think would have the most significant impact on Russian behavior?

**A.1.** Response not received in time for publication.

**Q.2.** *Sovereign Debt:* The Treasury Department's unclassified report on sovereign debt required by CAATSA noted that, "expanding sanctions could hinder the competitiveness of large U.S. asset managers and potentially have negative spillover effects into global financial markets and businesses."

What would be the impact on U.S. interests if we expanded sanctions to include dealings in new Russian sovereign debt and the full range of derivatives, with a transition period, and with certain explicit limits on the term of such debt? What would be the impact on global financial markets and businesses, and what suggestions do you have for mitigating any unintended consequences if we decide to go this route?

There have been articles, and concerns expressed by my colleagues (including at today's hearing) that Treasury and/or FinCEN have been delaying the production of material requested by Congress and possibly withholding information that was requested by Congress—and I mean in response to even bipartisan requests. You committed to provide further documents requested by the Intelligence Committee immediately, and to cooperate on this front. My colleague Senator Warner noted that Treasury is 7–8 months behind in some of these document requests. My questions to you are these:

Has Treasury or FinCEN ever intentionally delayed or withheld the production of material that was requested by Congress?

Has anyone at Treasury ever directed FinCEN to delay or withhold the production of material requested by Congress? If so, can you describe those circumstances, and the rationale for such action?

**A.2.** Response not received in time for publication.

**Q.3.** *Going After Putin Assets, and Those of His Cronies:* Leaving aside the diplomatic consequences, if we were to require of banks that they block Putin's personal assets, and those of his family members and close associates to whom he's transferred assets—like we did years ago with certain Iranians—given that they are often so well-hidden in layers of dummy corporations and anonymous en-

tities—would that have any real effect beyond the symbolic? I gather we have struggled to do this for many years, and he has hidden them well. But do we at least know who manages his assets for him, and could we not go after them with blocking or secondary bank sanctions? Why have we not done this already?

**A.3.** Response not received in time for publication.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR TOOMEY FROM SIGAL P. MANDELKER**

**Q.1.** Some European countries have expressed their opposition to the United States' withdrawal from the JCPOA.

The Treasury Department has indicated that on November 4, 2018, renewed sanctions on Iran will include those "on the provision of specialized financial messaging services to the Central Bank of Iran and Iranian financial institutions," per the Comprehensive Iran Sanctions and Divestment Act of 2010. These services include transactions on the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. Please explain, in unclassified terms, what will happen if the Treasury department is obligated to prohibit SWIFT transactions with the CBI and designated Iranian financial institutions but certain SWIFT member organizations elect to continue doing so.

What will be the effect of the European Commission's "blocking statute"—a mechanism Jean-Claude Juncker has said will "neutralize the extraterritorial effects of U.S. sanctions in the EU"—on European companies doing business with Iran?

Has this changed Treasury's view on the potential impact of sanctions on EU firms?

**A.1.** Response not received in time for publication.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR COTTON FROM SIGAL P. MANDELKER**

**Q.1.** Russia has recently embraced digital currencies, particularly Ethereum (see *https://cointelegraph.com/news/suddenly-vladimir-putin-meets-vitalik-buterin-endorses-ethereum*).

What can policymakers in the U.S. do to ensure that we are the leader in developing blockchain and digital currencies rather than Russia and China?

The SWIFT network facilitates cross-border payments through its vast messaging system. If the President wants to isolate Russia like Iran, is it true that the international SWIFT payments network based in Belgium can follow Europe and not unplug banks from those countries?

SWIFT and the EU's cooperation are needed to ensure sanctions involving cross-border payments are fully implemented (*https://www.axios.com/trump-administration-iran-sanctions-swift-financial-messaging-8fae6cd6-11c9-42a8-9d5b-6d3140a7ae83.html*). The next generation of payment infrastructure is likely to involve Blockchain and digital assets.

How can policymakers support American payment companies utilizing this technology to ensure this innovation develops here and aligns with our national security interests?

**A.1.** Response not received in time for publication.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM SIGAL P. MANDELKER**

**Q.1.** In the April 6th sanctions designations, Oleg Deripaska was designated pursuant to E.O. 13661 for having acted or purported to act for or on behalf of, directly or indirectly, a senior official of the Government of the Russian Federation, as well as pursuant to E.O. 13662 for operating in the energy sector of the Russian Federation economy.

As you gathered intelligence to build this sanctions package, did you examine Mr. Deripaska's interference in the United States?

Did you examine his relationship with Paul Manafort or other American citizens?

The United States has imposed sanctions on the FSB and GRU. Please describe the tangible impact of those sanctions.

How many FSB and GRU officers' accounts have been frozen?

How much money have these individuals lost access to as a result of these sanctions?

Have any FSB or GRU officer's property in the U.S. been seized as a result of these sanctions?

Please describe your dialogue with those American entities who invest in Russian sovereign debt. What specific measures have you taken to encourage U.S. entities to not invest in Russian sovereign debt?

**A.1.** Response not received in time for publication.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR TESTER FROM SIGAL P. MANDELKER**

**Q.1.** *Economic Effects of Sanctions:* What tools does the Department of Treasury use to measure the effectiveness of sanctions?

Specifically, what metrics does the Treasury utilize to indicate when sanctions have had their intended effect?

By these measures, have sanctions against Russia under the Countering America's Adversaries Through Sanctions Act (CAATSA) been successful?

**A.1.** Response not received in time for publication.

**Q.2.** *Money Laundering:* With the understanding that the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) has no criminal investigative or arrest authority, it has data analysis to support investigations and prosecutions of financial crimes, and refers possible cases to law enforcement authorities when it is warranted. FinCEN also submits requests for information to financial institutions from law enforcement agencies conducting criminal investigations and has the authority to issue civil money penalties.

Over the last 5 years, how many cases of money laundering has FinCEN referred to the Department of Justice or any other law enforcement authorities?

Out of those, how many have involved Russian nationals? Of those involving Russian nationals, how many were connected with U.S. individuals, LLCs or nonprofits?

**A.2.** Response not received in time for publication.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN FROM SIGAL P. MANDELKER**

**Q.1.** In the conference report attached to the Fiscal Year 2019 National Defense Authorization Act (NDAA), the Treasury Department, in coordination with other agencies, is directed to provide a briefing to Congress on the assets owned by Vladimir Putin, Russian business persons, and senior Russian Government officials, and their immediate family members and proxies. This briefing must include the location, value, size, and contents of their bank accounts, real estate holdings, and all other financial assets, and the shell companies they use to hide those assets.

When will you schedule this briefing?

Without disclosing intelligence sources and methods, would you consider publishing an unclassified report on the assets currently held by Putin, Russian business persons, senior Russian Government officials, and their immediate family members and proxies, and the companies they use to hide those assets, on a website of the Treasury Department? If yes, when can we expect Treasury to publish that unclassified report? If no, please explain why not.

During their press conference in Helsinki last month, Russian President Putin announced that he and President Trump "agreed to create the high-level working group that would bring together captains of Russian and American business."

Can you guarantee that no individual or entity under U.S. sanctions will be included in this working group of U.S. and Russian business leaders, if this working group is implemented? If not, please explain why not.

Based on the available information, do you believe that there is sufficient evidence to impose sanctions under existing U.S. law against Russian President Vladimir Putin personally?

If there is sufficient evidence, why has the Treasury Department not imposed sanctions on Vladimir Putin?

How many waivers have the Treasury Department granted for the Countering America's Adversaries Through Sanctions Act (CAATSA)? Please describe the parties for whom Treasury has granted such waivers.

Do you believe there is sufficient evidence to impose sanctions on the 12 Russian intelligence officers that the Justice Department indicted on July 13, 2018, for hacking the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC), and the presidential campaign of Hillary Clinton? If yes, does the Treasury Department intend to impose sanctions? If not, please explain why not.

The Commerce Department on July 29, 2018, granted Rusal America an exemption from aluminum tariffs imposed by President Trump. This exemption (exclusion) was reversed one day after I wrote to the Commerce Department on August 7, 2018. Commerce Department officials indicated that "they had coordinated with the [Office of Foreign Assets Control] in considering the Rusal application," and that OFAC "was ultimately the decider on whether sanctions should prevent approval of an exclusion."

Is this statement by the Commerce Department accurate?

Has the Commerce Department coordinated with OFAC or any other Treasury Department official regarding the eligibility of sanctioned companies generally for tariff exemptions?

Has the Commerce Department coordinated with OFAC or any other Treasury Department official regarding the eligibility of Rusal America for tariff exemptions?

Was OFAC "the decider" on whether Rusal America or any other sanctioned entity should be eligible to receive an exemption from the tariffs?

Did the Treasury Department play any role in the reversal of the Rusal America exemption on August 8, 2018? Please provide any and all documents in the Department's possession related to the July 9, 2018, or August 8, 2018, decisions on tariff exemptions for Rusal America.

**A.1.** Response not received in time for publication.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR DONNELLY FROM SIGAL P. MANDELKER**

**Q.1.** *Sanctions Effectiveness:* Ms. Mandelker, since the United States stepped up sanctions against Russia in 2014, sanctions have not changed or moderated the behavior of the Putin Government.

Are you currently holding back from taking enforcement actions against Russian entities or individuals that may currently be violating sanctions?

Do you have the staff and resources to implement and enforce an effective sanctions regime?

If provided, would additional staff and resources be used to implement and enforce existing sanctions, or to undertake additional enforcement actions?

**A.1.** Response not received in time for publication.

**Q.2.** *North Korea Sanctions Enforcement:* Ms. Mandelker, I am concerned that our hard work to strengthen North Korea sanctions has now gone to waste as Russia and China, among others, have relaxed their enforcement efforts. In the case of Russia, there are reports that it is still hiring North Korean workers and facilitating petroleum shipments.

Do you think that the sanctions pressure we are currently applying is sufficient to achieve our objective of ending North Korea's nuclear program?

Has Russia's and China's enforcement of North Korea sanctions improved, remained the same, or worsened since the President's summit in Helsinki?

What steps are you taking to ensure that both Russia and China are enforcing sanctions on North Korea?

**A.2.** Response not received in time for publication.

**Q.3.** *Sanctions on New Russian Sovereign Debt:* There are various pending legislative proposals to strengthen Russia sanctions, including proposals to sanction Russian sovereign debt and related derivatives. But Treasury has stated in the past that such sanctions could negatively impact U.S. investors.

Do you think that sanctions on new Russian sovereign debt and related derivatives will help to change Putin's calculus?

Do you think that the EU would be open to implementing similar actions?

As a last resort strategy, some have referred to sovereign debt sanctions as the "nuclear option". Do you support that conclusion, that sanctioning sovereign debt would only be considered after all else fails?

**A.3.** Response not received in time for publication.

**Q.4.** *Beneficial Ownership and Corporate Transparency:* Many reports have concluded that the U.S. is among the easiest countries to create an anonymous shell company. As a result, corrupt oligarchs and rogue Nations can often exploit our vulnerabilities to evade sanctions and move money through the U.S. as a legal business entity.

To what extent have Russian officials utilized shadow companies to access the U.S. financial system?

Do the use and exploitation of anonymous shell companies negatively impact our national security?

Would legislation requiring corporate beneficial ownership transparency increase your ability to effectively apply sanctions against corrupt oligarchs and officials?

In May, FinCEN implemented its Customer Due Diligence (CDD) Rule to require financial institutions to identify the beneficial owner of legal entity customers. The CDD rule will be helpful going forward, but it is not retroactive for existing accounts.

What is the expected impact of the CDD rule on beneficial ownership disclosure?

What additional steps must the United States take to eliminate the glaring systemic vulnerability of anonymous shell companies that criminals and corrupt foreign officials exploit to move money through the financial system?

**A.4.** Response not received in time for publication.

---

## RESPONSES TO WRITTEN QUESTIONS OF SENATOR SCHATZ FROM SIGAL P. MANDELKER

**Q.1.** Is the U.S. Government committed to deterring and, if necessary, punishing foreign interference in the democratic election, processes, or institutions of a treaty ally, political ally, or partner Government of the United States?

If yes, describe the tools that are available to the U.S. Government to prevent and punish foreign interference in ally and partner Governments in Europe and Eurasia, including the existing sanctions authorities that the U.S. Government can levy against individuals or organizations suspected of foreign interference.

How does the U.S. Government coordinate with NATO allies and the Governments of other political allies and partners to share information about suspected foreign interference in democratic elections, processes, or institutions?

What mechanisms exist for the U.S. Government to gather information from NATO allies and the Governments of other political allies and partners about individuals and organizations responsible

for foreign interference in democratic elections, processes, or institutions overseas?

Describe how, if at all, the U.S. Government currently makes decisions with NATO allies and the Governments of other political allies and partners to take actions to punish individuals or organizations for foreign interference in democratic elections, processes, or institutions overseas.

Does the U.S. Government face any limitations with coordinating with NATO allies and the Governments of other political allies and partners as it relates to deterring suspected individuals or organizations from or punishing them for foreign interference in democratic elections, processes, or institutions overseas?

If yes, what recommendations would you make to Congress to ensure that the U.S. Government has sufficient authority to coordinate with appropriate foreign Governments concerning election interference?

**A.1.** Response not received in time for publication.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM CHRISTOPHER KREBS**

**Q.1.** Ongoing Russian cyberattacks on the U.S. have been widely reported—as your testimony notes, Homeland Security has issued warnings on Russian attempts to penetrate critical infrastructure, targeting organizations in the business, energy, nuclear, water, aviation, and manufacturing sectors. The alerts describe "multistage intrusion campaigns" which allowed remote access to U.S. energy sector networks, including the control systems for energy generation facilities. As you said, "we are facing an urgent, evolving crisis in cyberspace. Our adversaries' capabilities online are outpacing our stovepiped defenses."

Can you describe the nature and scale of these attacks, their intensity, purposes, and key targets? Are they deploying malware for future use? Reconnaissance? Testing our system security? Do we think they could actually take control of any utility plants?

**A.1.** Since at least March 2016, Russian Government cyberactors have targeted Government entities and multiple U.S. critical infrastructure sectors, including energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. The U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) characterize this activity as a multistage intrusion campaign by Russian Government cyberactors who targeted small commercial facility networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian Government cyberactors conducted network reconnaissance, moved laterally, and collected information pertaining to industrial control systems, or the operational technology that operates our Nation's critical infrastructure.

While significant and concerning, the activity identified in these incidents did not put these malicious cyberactors in a position to take control of utility plants. Additional information on this activity can be found in the joint technical alert by DHS and FBI, found online at: *https://www.us-cert.gov/ncas/alerts/TA18-074A*.

**Q.2.** Are your efforts to eliminate the stovepipe problem and better coordinate, both within the U.S. Government, and between the Federal Government and State and local governments, enough to defeat them?

**A.2.** To break down information stovepipes and ensure cross-sector approaches to protecting our Nation, the Department's specific cybersecurity authorities executed through NPPD—including authorities related to sharing, analyzing, and coordinating actionable information related to cybersecurity risks and incidents; protecting Federal information systems; and responding to cybersecurity incidents—enable NPPD to engage with Federal and non-Federal entities (i.e., all stakeholders—public, private, and international) and across and beyond all critical infrastructure sectors to collaboratively improve cybersecurity practices and protect Federal and non-Federal entities from cyber-risks.

The Homeland Security Act of 2002, and following amendments, as well as Executive Branch policies, have centralized functions of the Federal Government focused on protecting critical infrastructure at the Department of Homeland Security (DHS). The Homeland Security Act was amended in 2014 and 2015 to codify the role of the Department's National Cybersecurity and Communications Integration Center (NCCIC) as the Federal–civilian interface for sharing information regarding cybersecurity risks and incidents and authorize the NCCIC to provide cybersecurity related technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities. In a similar fashion, the Cybersecurity Act of 2015 also establishes the NCCIC as the Federal Government's central hub for sharing cyberthreat indicators between the private sector and the Federal Government and requires the Department to establish the Federal Government's capability and process for sharing cyberthreat indicators with both Federal and non-Federal entities.

Cross-sector centralization and coordination of the Federal Government's cybersecurity efforts is critical to our Nation's national security, economic security, and public health and safety. Information regarding cybersecurity threats, vulnerability, and incidents must be shared as quickly as our adversaries move in cyberspace.

---

## RESPONSES TO WRITTEN QUESTIONS OF SENATOR MORAN FROM CHRISTOPHER KREBS

**Q.1.** The Federal Information Security Modernization Act of 2014 (FISMA) expanded and clarified the Department of Homeland Security's (DHS) responsibilities in implementation and oversight of information security at other Federal agencies upon enactment, including the authority to develop, issue, and oversee agencies' implementation of "binding operational directives," or BODs. With examples of BODs spanning from requiring agencies to participate in risk assessments to outright banning the use of Kaspersky Lab equipment, it is important for Congress to understand DHS's decision-making and oversight processes.

First, please describe how DHS identifies the necessary conditions to issue a BOD.

How does DHS establish and maintain oversight of agencies' implementation of the BOD?

Does DHS have the necessary authorities and capability to ensure accountability of BOD implementation across diverse agencies?

How does DHS measure the effectiveness of the BOD?

Ultimately, how are BODs integrated in a comprehensive cybersecurity strategy?

**A.1.** The Secretary of the U.S. Department of Homeland Security (DHS), in consultation with the Director of the Office of Management and Budget (OMB), has the authority under 44 U.S.C. §3553(b)(2) to develop and oversee the implementation of binding operational directives (BOD). The Federal Information Security Modernization Act (FISMA) includes specific topics for BODs, including requirements for reporting security incidents to DHS's National Cybersecurity and Communications Integration Center (NCCIC), requirements for the contents of the annual FISMA reports, requirements for the mitigation of exigent risks to information systems, and other operational requirements as OMB, or DHS in consultation with OMB, may determine are necessary.

DHS, acting through the National Protection and Programs Directorate (NPPD), identifies risks or requirements to be addressed through BODs. DHS also accepts ideas for potential BODs from entities, such as the Federal Chief Information Officer (CIO) Council, independent security researchers, or other partners. As needed, DHS may convene a group of subject matter experts from Federal agencies, OMB, and the National Institute of Standards and Technology to consider the relative merits of particular risks in order to determine the appropriateness of a given BOD or determine the prioritization of different BODs.

Generally, when determining whether a certain issue is appropriate for a BOD, DHS considers the following questions:

- Is the proposed BOD related to an active threat? If so, what is the scope and magnitude of the problem?
- Is the proposed BOD related to a potential identified risk?
- What category/schedule does the potential BOD fit into (planned, escalation of issue, or emergency)?
- Is this issue specific to a particular Federal agency or could it be applicable across the civilian Federal executive branch?
- What is the difficulty to exploit the vulnerability?
- Is the issue/subject sensitive or classified?
- Are external events or threat intelligence driving the need for or request of the proposed BOD?
- Can the proposed BOD be measured and validated by DHS?
- Could the issue or threat be addressed satisfactorily and fully through other mechanisms?
- Has DHS socialized the proposed BOD subject with applicable stakeholders, such as CIO/Chief Information Security Officer (CISO) councils?
- What is the end state of proposed BOD?

- What other operational requirements have been issued by way of policy, guidance, and standards in relation to this BOD?
- Does the BOD address or reemphasize Federal program such as Continuous Diagnostics and Mitigation, EINSTEIN, automated indicator sharing, etc.?
- Is this BOD associated with the requirements for the content of the annual reports required to be submitted by Federal agencies?
- Is this BOD associated with the requirements for reporting incidents to the NCCIC?
- Is there another action that would be more effective than a BOD?

DHS has found its current authorities to be effective at coordinating and driving the timely response and implementation of specific BOD requirements but acknowledges that, under certain circumstances, DHS will be unable to ensure implementation at the agency-level unilaterally. DHS ensures Federal agency compliance with BODs using several methods. First, BODs have historically been issued by the Secretary to Federal agency leadership as high-priority items, and their implementation status is followed closely by DHS's senior leadership. When implementation issues arise, DHS engages with Federal agency CIOs and CISOs. If the agency continues not to comply, DHS leadership may engage with his or her counterpart at a noncompliant agency. When additional attention is needed, DHS may work with OMB. Ultimately, the Secretary or Deputy Secretary may, at their discretion, contact their counterparts at each noncompliant agency.

DHS measures BOD effectiveness based on the completion of all required tasks by agencies, along with achieving the stated, desired end state which is defined by eliminating or adequately addressing the identified risk. Throughout the development of a BOD, required actions on the part of agencies are determined to ultimately minimize or eliminate the risk posed by previously identified vulnerabilities. For instance, in 2015 the Secretary directed agencies to promptly patch known vulnerabilities on their Internet-facing systems. Agencies have responded quickly in implementing the Secretary's BOD and have sustained this progress. When the Secretary issued this BOD, NPPD identified more than 360 "stale" critical vulnerabilities across Federal civilian agencies, which means the vulnerabilities had been known for at least 30 days and remained unpatched. Since December 2015, NPPD has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly.

Consistent with the Department's cybersecurity strategy, BODs have addressed cybersecurity priorities requiring immediate attention and mandatory action by Federal agencies to protect Federal information and information systems. It is important to note that BODs are just one tool DHS has at its disposal to ensure Federal agencies and their associated networks are adequately and properly protected.

**Q.2.** Your written testimony described the joint efforts of DHS and the Federal Bureau of Investigation (FBI) to identify practices of

Russian Government actors targeting certain entities that eventually become "pivot points" to leverage access to major, high-value assets operating the Nation's infrastructure.

What have been some of the priority recommendations that DHS and FBI have provided network defenders to reduce exposure to this malicious, yet strategic, exposure?

**A.2.** Since at least March 2016, Russian Government cyberactors have targeted Government entities and multiple U.S. critical infrastructure sectors, including energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. The U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) characterize this activity as a multistage intrusion campaign by Russian Government cyberactors who targeted small commercial facility networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian Government cyberactors conducted network reconnaissance, moved laterally, and collected information pertaining to industrial control systems, or the operational technology that operates our Nation's critical infrastructure.

Additional information on this activity can be found in the joint technical alert by DHS and FBI, found online at: *https://www.uscert.gov/ncas/alerts/TA18-074A.*

Recommendations provided to network defenders include monitoring for known indicators of compromise, active defense for spearphishing and watering hole intrusion vectors, blocking all outbound server message block network traffic, requiring the use of multifactor authentication for all external interfaces, use of malware signatures, and other recommended courses of action provided within the technical alert.

**Q.3.** Your written testimony mentions the collaborative efforts of DHS with private industry actors to improve assessment, detection, protection, and mitigation of cyberthreats, including Executive Order 13800.

What are some of the best examples of public–private partnerships that the agency has been a part of (that you are able to share with this Committee)? What exactly were those partnership able to achieve?

**A.3.** Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, recognizes that effective cybersecurity requires entities to identify, detect, respond, and, when necessary, recover from cyberintrusions. Through outreach to stakeholders, the U.S. Department of Homeland Security (DHS) is sharing cybersecurity threat information and assisting with the prioritization and mitigation of cybersecurity risks.

DHS leads efforts to defend our Nation's critical infrastructure from cyberthreats. Today's infrastructure is more complex and dynamic with interdependencies that increase the challenge of reducing risk and ensuring resiliency. DHS not only shares unclassified and classified cyberthreat information as well as providing a full range of technical assistance capabilities, but also closely coordinates with our Federal partners, including intelligence agencies, law enforcement, and sector-specific agencies.

The National Cybersecurity and Communications Integration Center (NCCIC) fosters a strong network of trusted global partnerships. The NCCIC routinely collaborates with these trusted partners to share information, coordinate actions, conduct analysis, and develop common processes and joint plans. The NCCIC offers a portfolio of no-cost products and services organized around its core functions. Some examples include the Industrial Controls Systems Joint Working Group to facilitate information sharing and to reduce the cyber-risk to the Nation's industrial control systems; the Cyber Information Sharing and Collaboration Program enables actionable, relevant, and timely unclassified information exchange through trusted public–private partnerships across all critical infrastructure sectors; the automated indicator sharing capability enables the exchange of cyberthreat indicators between and among the Federal Government and the private sector at machine speed; and the Enhanced Cybersecurity Services is an intrusion detection and prevention capability that is available to U.S.-based entities and State, local, tribal, and territorial government organizations.

**Q.4.** With the support of the Administration and colleagues from both sides of the aisle, I was successful in getting the Modernizing Government Technology (MGT) Act signed into law as part of the National Defense Authorization Act for FY2018. The law addresses the foundational cybersecurity threats that outdated legacy systems in our Federal agencies pose.

Would you agree that outdated, unsupported legacy IT systems pose a serious threat to the information security of our Federal agencies?

**A.4.** Yes, the challenges posed by outdated, end-of-life (EOL), legacy Federal information technology systems create serious risks to the information security of our Federal agencies. For instance, the issue has been apparent in the implementation of the U.S. Department of Homeland Security's (DHS) Binding Operational Directives (BOD). As an example, during the implementation of BOD 15-01 (Mitigating Critical Vulnerabilities) and BOD 16-02 (Securing Network Infrastructure Devices), DHS identified and monitored dozens of EOL systems. Some legacy systems could no longer be patched, others were not supported by the vendor, and some experienced significant performance issues if not reconfigured during the security upgrade and enhancement process. Most legacy systems are simply not designed for the current environment and the need for modern security approaches. Fortunately, in most cases, DHS and the agency were able to address these issues and either upgrade, transition, or mitigate.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR TESTER FROM CHRISTOPHER KREBS**

**Q.1.** Please provide a detailed list of what DHS has taken to date in order to improve election security in the State of Montana since the 2016 election cycle.

**A.1.** The U.S. Department of Homeland Security (DHS) engages with non-Federal entities, such as the State of Montana, to share cybersecurity information and provide technical assistance on a vol-

untary basis. Successful voluntary partnerships require trust and confidentiality. As such, DHS generally defers to individual entities to respond to questions regarding details of an incident or steps that an entity may have taken to mitigate vulnerabilities.

**Q.2.** To the best of your knowledge, has the State of Montana implemented any of the suggested election security improvements offered by DHS?

**A.2.** As noted in the previous response, DHS generally defers to individual entities to respond to questions regarding details of an incident or steps that an entity may have taken to mitigate vulnerabilities.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM CHRISTOPHER A. FORD**

**Q.1.** *CAATSA Implementation:* Many of us on both sides have repeatedly urged more assertive implementation of mandatory sanctions under CAATSA, in order to deter further Russian attacks. I know you have begun to do a bit more in recent months, and in some cases would prefer to use EO authorities because you see them as more flexible. But there is still a lot more that could be done with mandatory CAATSA sanctions.

Can you give us a more precise sense of what you have planned before the elections to signal more powerfully to Russia's leaders that they must stop—and what you are preparing for generally, in terms of escalation, if the Russians continue their aggressive actions through the elections and beyond?

**A.1.** The Department of State has made it clear to the Russian Government at the highest levels that any efforts to interfere in the 2018 midterm elections will not be tolerated and will be met with severe consequences. While the Department's mandate is to lead on foreign policy, we will continue to support the efforts of the Departments of Homeland Security and Justice—and, as appropriate, State and local officials—to secure our elections, leveraging all necessary and available Department resources and tools to counter Russian malign influence.

**Q.2.** What are the general sanctions areas—banking, energy, sovereign debt, sectoral sanctions, or a mix of all of them—that you think would have the most significant impact on Russian behavior?

**A.2.** We have robust sanctions authorities at our disposal, which we are using in close coordination with our allies and partners to impose costs on Russia for the entirety of its malign behavior. Sanctions are a powerful foreign policy tool, and are most impactful when used in coordination with allies and partners to maximize their effectiveness. Sanctions have the strongest impact when tied to a clear foreign policy goal, and used in tandem with diplomatic outreach. Providing the State Department with flexibility in implementation allows us to engage with allies, maintain unity, and maximize sanctions pressure on Russia. For example, the threat of sanctions under CAATSA Section 231 has prompted other States to abandon billions of dollars in planned or announced arms deals with Russia, imposing additional financial costs on the Russian

Government. As a result, Russia has fewer resources with which to finance its influence campaigns.

**Q.3.** *Maintaining Multilateral Support for Sanctions:* It's clear that enlisting other countries in our efforts to push back on Russian aggression—including countries like France, Germany, Britain, the Baltic States, and others who have been victimized by Russian aggression—is critical. They also have a huge stake in ensuring Russia abides by international law in Crimea and Ukraine, and in protecting their own elections and infrastructure systems.

Can you describe precisely what we are doing to enlist the support of other countries in our efforts to impose real costs on continuing Russian aggression across the board, in all these areas?

**A.3.** We work closely with partners and allies to respond to Russian aggression, share best practices, expose Russian campaigns and tactics, and build collective resilience. We work both on a bilateral and multilateral basis to achieve these goals. For example, the coordinated expulsion of Russian officers from 28 countries and NATO in response to the Salisbury attack on Sergei and Yulia Skripal sent a strong message to Russia that its destabilizing and brazen activity will not be tolerated by the international community. Additionally, we support multilateral efforts to share information and build collective resilience, such as at the European Center for Countering Hybrid Threats in Helsinki. We have exposed Russian malicious cyberactivity publicly, in concert with partners.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR TOOMEY FROM CHRISTOPHER A. FORD**

**Q.1.** Some European countries have expressed their opposition to the United States' withdrawal from the JCPOA.

The Treasury Department has indicated that on November 4, 2018, renewed sanctions on Iran will include those "on the provision of specialized financial messaging services to the Central Bank of Iran and Iranian financial institutions," per the Comprehensive Iran Sanctions and Divestment Act of 2010. These services include transactions on the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. Please explain, in unclassified terms, what will happen if the Treasury department is obligated to prohibit SWIFT transactions with the CBI and designated Iranian financial institutions but certain SWIFT member organizations elect to continue doing so.

What will be the effect of the European Commission's "blocking statute"—a mechanism Jean-Claude Juncker has said will "neutralize the extraterritorial effects of U.S. sanctions in the EU"—on European companies doing business with Iran?

Has this changed Treasury's view on the potential impact of sanctions on EU firms?

**A.1.** Response not received in time for publication.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR COTTON FROM CHRISTOPHER A. FORD**

**Q.1.** Russia has recently embraced digital currencies, particularly Ethereum (see *https://cointelegraph.com/news/suddenly-vladimir-putin-meets-vitalik-buterin-endorses-ethereum*).

What can policymakers in the U.S. do to ensure that we are the leader in developing blockchain and digital currencies rather than Russia and China?

**A.1.** The Department of State is closely monitoring both the development and deployment of this technology. U.S. private sector companies have made the United States a global leader in this emerging technology. Supporting a strong and open U.S. innovation ecosystem, pursuing promarket approaches, removing barriers to innovation, and preserving the freedom to pursue new ideas and business models will allow us to continue to lead blockchain innovation now and in the future. In contrast to State-led national planning for technological development, our light-touch and flexible approach allows the best technical solutions to succeed in the marketplace, while our multistakeholder approach to policymaking also ensures that all viewpoints can be taken into account.

**Q.2.** The SWIFT network facilitates cross-border payments through its vast messaging system. If the President wants to isolate Russia like Iran, is it true that the international SWIFT payments network based in Belgium can follow Europe and not unplug banks from those countries?

**A.2.** We consistently review all components of the international banking system, including developing payment infrastructures. We are closely engaged with our European allies in finding a way forward to end Russia's destabilizing behavior. Transatlantic unity is the cornerstone of our sanctions against Russia. Providing the State Department with flexibility in implementation allows us to engage with allies, maintain unity, and maximize sanctions pressure on Russia.

We have robust sanctions authorities at our disposal. We are using these authorities in close coordination with our allies and partners to impose costs on Russia for the entirety of its malign behavior.

**Q.3.** SWIFT and the EU's cooperation are needed to ensure sanctions involving cross-border payments are fully implemented (*https://www.axios.com/trump-administration-iran-sanctions-swift-financial-messaging-8fae6cd6-11c9-42a8-9d5b-6d3140a7ae83.html*). The next generation of payment infrastructure is likely to involve Blockchain and digital assets.

How can policymakers support American payment companies utilizing this technology to ensure this innovation develops here and aligns with our national security interests?

**A.3.** The U.S. Government encourages the development of new technologies by our innovative private sector. Innovation and creativity are the hallmarks of our private sector and U.S. industry has continually shown the ability to adopt new technologies to drive economic growth. Blockchain technology has potential to help U.S. industry in several areas including securing transactions, sup-

ply chain management, and the financial sector, just to name a few. We will continue to monitor the development of and the private sector's applications of this innovative technology.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM CHRISTOPHER A. FORD**

**Q.1.** The FY2019 National Defense Authorization Act includes a reporting requirement in Section 1294(c) regarding executive branch sanction determinations under Section 231 of CAATSA. Do I have your commitment that this report will be delivered to Congress on or before the 90-day deadline mandated in the law?

**A.1.** The law requires the report to be submitted by the President. I am committed to providing the President or his delegate whatever information and support is needed to prepare and submit the report as required by law.

**Q.2.** Can you put a dollar amount on the Russian arms deals that you have been able to turn off as a result of Section 231?

**A.2.** We estimate that we have so far deterred several billion dollars in Russian arms deals as a result of our Section 231 implementation efforts.

**Q.3.** Secretary Mattis was an ardent supporter of the new CAATSA waiver language with respect to Section 231 that was included in the FY2019 National Defense Authorization law. Has he also supported State's efforts to wean Governments from purchasing Russian equipment? If so, how has he specifically supported your efforts?

**A.3.** Secretary Mattis has been a strong voice in encouraging partner countries to end defense relationships with Russia and to seek an alternative source of supply. I refer you to the Department of Defense for any additional details on Secretary Mattis' efforts.

**Q.4.** How specifically has the State Department engaged and coordinated with the Defense Department on discouraging all significant transactions with the Russian defense industry?

**A.4.** The Defense Department is an integral part of the interagency process for implementing CAATSA Section 231. We coordinate with the Defense Department on our engagement with partners and allies related to CAATSA Section 231.

**Q.5.** On August 24, A.A. Mikheev, the Director General of Rosoboronexport said that contracts were under negotiation with India on the S-400 air defense system, 48 Mi-17 helicopters, and joint production of KA-226T helicopters. Do you assess that these contracts are indeed under negotiation?

**A.5.** We are aware of the public reporting on this issue but will not speculate on the status of any deals that may be the subject of discussions between Russia and India. We have discussed CAATSA Section 231 extensively with the Government of India, and the United States is working with all partner and allied countries, including India, to discourage them from engaging in major defense purchases from Russia.

**Q.6.** Do you assess that India and Rosobornexport are negotiating contracts for other defense equipment, not mentioned above?

**A.6.** I cannot speculate on the status of any further deals that may be the subject of discussions between Russia and India. However, we are aware that Russia is actively and publicly seeking to undermine U.S. sanctions, including by continuing to actively market weapons systems and other military equipment around the world. With regard to India, our focus is on discouraging them from engaging in major defense purchases from Russia.

**Q.7.** If these contracts and transfers are completed, how do you assess they will affect U.S. defense cooperation with India, which the Pentagon reports has increased to significant levels in recent years?

**A.7.** Our focus is on encouraging all partner and allied countries, including India, to not engage in sanctionable activity, so as to avoid the need for the imposition of sanctions under CAATSA 231. I cannot comment specifically on how U.S. defense cooperation with India will be affected if these purported transactions are completed.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SCHATZ FROM CHRISTOPHER A. FORD**

**Q.1.** Is the U.S. Government committed to deterring and, if necessary, punishing foreign interference in the democratic election, processes, or institutions of a treaty ally, political ally, or partner Government of the United States?

**A.1.** Yes. The Department works closely with partners and allies to build collective resilience, share best practices, and respond to Russian attempts to interfere in democratic processes and institutions. The Administration has made it clear that such interference is unacceptable.

**Q.2.** If yes, describe the tools that are available to the U.S. Government to prevent and punish foreign interference in ally and partner Governments in Europe and Eurasia, including the existing sanctions authorities that the U.S. Government can levy against individuals or organizations suspected of foreign interference.

**A.2.** The Department is committed to responding to Russian aggression, including its malign influence campaigns, and is committed to utilizing political, economic, diplomatic, and law enforcement tools in response. Since January 2017, the Trump administration has sanctioned 229 individuals and entities in Russia in response to its destabilizing behavior. We are also focused on leveraging our public diplomacy, foreign assistance, and diplomatic resources to improve the resilience of our partners and allies, as well as on sharing best practices and supporting multilateral efforts to build up our collective defenses.

**Q.3.** How does the U.S. Government coordinate with NATO allies and the Governments of other political allies and partners to share information about suspected foreign interference in democratic elections, processes, or institutions?

**A.3.** We work closely with NATO allies to share information regarding Russian aggression. This includes discussing best prac-

tices, exposing Russian disinformation campaigns and tactics, and building collective resilience. Additionally, we support broader multilateral efforts to share information and build resilience, such as at the European Center of Excellence for Countering Hybrid Threats in Helsinki. We also work to expose Russian malicious cyberactivity publicly, in concert with allies.

**Q.4.** What mechanisms exist for the U.S. Government to gather information from NATO allies and the Governments of other political allies and partners about individuals and organizations responsible for foreign interference in democratic elections, processes, or institutions overseas?

**A.4.** NATO allies share information on common threats with each other on a regular basis. At the Warsaw Summit in July 2016, Heads of State and Government agreed to establish a new Joint Intelligence and Security Division (JISD), which merges civil and military intelligence functions in order to improve NATO's ability to draw on a wide range of intelligence resources. JISD, led by the Assistant Secretary General for Intelligence and Security, has improved NATO's ability to facilitate timely and relevant support to Allied decision-making and operations, particularly on terrorism, hybrid warfare, and cyberthreat issues.

**Q.5.** Describe how, if at all, the U.S. Government currently makes decisions with NATO allies and the Governments of other political allies and partners to take actions to punish individuals or organizations for foreign interference in democratic elections, processes, or institutions overseas.

**A.5.** At the NATO Summit in Brussels, we joined our NATO allies in affirming our shared concerns regarding threats from State and non-State actors who use hybrid activities that aim to create ambiguity and blur the lines between peace, crisis, and conflict. While NATO allies acknowledge that the primary responsibility for responding to hybrid threats rests with the targeted Nation, NATO stands ready, upon decision by the North Atlantic Council, to assist an Ally at any stage of a hybrid campaign. In Brussels allies announced the establishment of counterhybrid support teams, to provide tailored, targeted assistance to allies, upon their request, in preparing for and responding to hybrid activities.

**Q.6.** Does the U.S. Government face any limitations with coordinating with NATO allies and the Governments of other political allies and partners as it relates to deterring suspected individuals or organizations from or punishing them for foreign interference in democratic elections, processes, or institutions overseas?

**A.6.** The Department works closely with partners and allies to build collective resilience, share best practices, and respond to Russian attempts to interfere in democratic process and institutions. We utilize bilateral and multilateral engagements to coordinate efforts and response with partner Governments and NATO allies. There are no institutional limitations on this coordination.

**Q.7.** If yes, what recommendations would you make to Congress to ensure that the U.S. Government has sufficient authority to coordinate with appropriate foreign Governments concerning election interference?

**A.7.** Transatlantic unity is the cornerstone of our sanctions against Russia; providing the State Department flexibility in implementation allows us to engage with allies, maintain unity, and maximize sanctions pressure on Russia.

**Q.8.** Describe the U.S. Government's interpretation of its commitment to protect the political independence of NATO members, as it relates to the North Atlantic Treaty of 1949.

**A.8.** Maintaining such independence lies at the core of the Alliance, and the Washington Treaty obliges all allies to advance and defend the institutions that guarantee such independence. Under Article 2 of the Treaty, all allies commit to "contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which those institutions are founded, and by promoting conditions of stability and well-being." Article 4 provides that the allies shall consult if, "in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened." And in the event that such independence is threatened by means of an armed attack, Article 5 States that "the parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." In such case, each Party is obligated to "assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force."

The President, Vice President, Secretaries of State and Defense, and the Chairman of the Joint Chiefs of Staff have all reiterated that the U.S. commitment to these treaty obligations is ironclad. If allies agree that an armed attack has occurred within the meaning of Article 5, the United States will adhere to our treaty commitments and respond as appropriate with our NATO allies.

**Q.9.** In your view, would NATO's collective defense commitment to protect the political independence of member States be better served with an affirmative policy that treats foreign interference in the democratic election, processes, or institutions of one member as an effort to undermine the political independence of all members and their democratic institutions?

**A.9.** Article 4 of the Washington Treaty provides that the allies shall consult when, "in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened" in any manner, and the United States welcomes consultation with allies in such circumstances. The specific collective defense obligation of Article 5, however, is only activated in response to an armed attack. Over the past 69 years since the Alliance was formed, the allies' understanding of what could constitute an armed attack has included terrorism, cyberattacks, and hybrid attacks. A precise determination would depend on the specific facts at hand, and be made collectively by all the allies.

**Q.10.** If yes, would the Administration support an effort to develop a multinational sanctions regime under NATO to impose punishment on individuals or organizations suspected of interfering in the

democratic election, processes, or institutions of any NATO member?

**A.10.** While primary responsibility for this issue within the Department of State rests with EUR Assistant Secretary A. Wess Mitchell, the Under Secretary for Political Affairs, and Secretary Pompeo, my understanding is that, if requested by an Ally under Article 4, the United States would welcome an opportunity to consult with allies regarding an appropriate response.