

**ANNUAL WORLD WIDE THREATS HEARING WITH  
HEADS OF THE INTELLIGENCE COMMUNITY**

**Thursday, March 9, 2023**

**U.S. House of Representatives,**

**Permanent Select Committee on Intelligence,**

**Washington, D.C.**

The committee met, pursuant to call, at 10:01 a.m., in Room 210, Cannon House Office Building, the Honorable Michael R. Turner [chairman of the committee] presiding.

Present: Representatives Turner, Wenstrup, Stewart, Crawford, Stefanik, Kelly, LaHood, Fitzpatrick, Gallagher, Scott, Hill, Crenshaw, Waltz, Garcia, Himes, Carson, Krishnamoorthi, Crow, Bera, Gottheimer, Gomez, and Spanberger.

The Chairman. The committee will come to order.

Good morning. Appreciate you all being here.

Before we start, I want to address some housekeeping matters.

First, today's open portion is being broadcast live and streamed on the committee's YouTube channel. It will be conducted entirely on an unclassified basis. All participants are reminded to refrain from discussing classified or other information protected from public disclosure.

It is my privilege to welcome a distinguished panel of leaders to our hearing today to discuss the Intelligence Community's Annual Threat Assessment.

During today's proceedings, we will hear from Lieutenant General Scott Berrier, Director of the Defense Intelligence Agency; the Honorable William Burns, Director of the Central Intelligence Agency; the Honorable Avril Haines, Director of National Intelligence; General Paul Nakasone, Director of the National Security Agency; and the Honorable Christopher Wray, Director of the Federal Bureau of Investigation.

Thank you all for your service and for your appearance here today.

I also want to thank all of our committee members for their cooperation today. We will have both open and closed sessions with our witnesses. Our plan is to complete the open session by noon, adjourn for a lunch break, and resume in closed session.

Now, to my opening statement.

This is our annual hearing on worldwide threats. It is an opportunity for the Intelligence Community to come before Congress and the American people to talk about the threats that our Nation faces. It also will be an opportunity for us to talk about how we can respond to those threats and what are the needs of the Intelligence Community.

Our adversaries self-select, and today you will certainly hear about China, Russia,

North Korea, Iran, and others. We will also be discussing issues about domestic violent extremist groups. Domestic violent extremist groups, such as antifa, have funding; organizational structures, which include communications, training, logistics; illegal activities, especially, as we have seen across the country, violence.

Today, when we discuss the Intelligence Community's surveillance of domestic violence extremist organizations, we are certainly going to be discussing the issue of our concerns of the rights of everyday, law-abiding Americans whose rights may be violated.

Since 1977, our committee was formed to respond to abuses by the Intelligence Community. We were organized to protect the integrity of our laws, to protect our citizens' constitutional rights. Foremost, that is why our committee is here. Concurrently, we are also here to protect our national security, to protect our country and its citizens from foreign and domestic adversaries.

Now, I want to welcome you to our new Intelligence Community. It is new because we have a renewed commitment of both bipartisanship and working in a professional manner. Our committee was opened by an address by the Speaker of the House and by Minority Leader Jeffries, where he tasked each and every member of our committee to be dedicated to national security and to working together. I am very pleased that Jim Himes and myself, my ranking member, are dedicated to that bipartisan cooperation and to the professionalism.

No one is served by members of this committee fighting with each other. We are here to work together. That is what the American people deserve and what the American people expect. And we will not always agree, but through debate and dialogue, we will find solutions.

One of these issues that will be open for debate -- open for debate -- is the renewal of 702 of FISA, the Foreign Intelligence Surveillance Act, Section 702.

702 is essential. It has provided successes, and it has provided those successes

against our adversaries. However, there have been and there continue to be many abuses of FISA. It must be reformed.

Our first step is that we must be honest with the American people. Today, I am going to be looking to each of you for honesty and acknowledgement that FISA has been abused. From that acknowledgement, we can together find solutions and reforms as we work to renew 702 of FISA.

To aid in this process, I have appointed a working group, three members of the majority. Jim Himes will be appointing three members of the minority to the working group. The working group will have equal numbers of Democrats and Republicans. Darin LaHood will be its chair.

I have appointed Representative Darin LaHood to chair this working group because of his leadership, expertise, and integrity. Prior to his election to Congress, Darin LaHood served as a career prosecutor at both the State and the Federal levels. Specifically, he worked for the U.S. Department of Justice as an assistant United States attorney and was selected as the chief terrorism prosecutor in Las Vegas, Nevada. I am confident that his experience in investigating and prosecuting criminal and terrorist activities make him supremely qualified to lead this important bipartisan working group.

I am excited about the important work this working group is planning to do, and, under Darin's leadership, I am confident that they will produce meaningful reform proposals. But I would be remiss if I did not underscore the burdensome task that they have in front of them and the reality that Congress cannot preserve FISA alone.

What we need from each of you is a commitment to work with the committee and Representative LaHood's working group to gain America's trust and to pursue legislative reforms to the FISA process that safeguard and guarantee the constitutional rights of all American citizens.

This commitment is necessary because it is the actions of individuals in your organizations who have degraded the public trust and has ultimately put FISA at risk. It is not Congress that has put FISA at risk. It is your organization. These things, these abuses, did not happen somewhere else. They happened underneath the leadership of the individuals that are represented at the table in front of us.

Now, that may sound harsh, but the first step in earning back this trust is an ability to admit that there is, in fact, a problem. This problem can't be explained as unintentional line-staff mistakes and misunderstandings. It is a problem that will require cooperation, with clear and open minds.

We cannot undertake a clean reauthorization of 702 without an acknowledgement of the problem, a concerted effort to gain back trust, and a commitment to working with Congress toward meeting more reforms.

I know that every member of this committee is committed to pursue the renewal of 702 and understand its importance and the work that it accomplishes for our national security.

With that, I yield to my ranking member.

Mr. Himes. Thank you, Mr. Chairman.

And thank you to each of our witnesses for appearing today. We are grateful for the important work that the Intelligence Community workforce does every day for our Nation.

The annual worldwide threats open hearing is a unique opportunity for the public to hear directly from Intelligence Community leadership about the latest assessments of the most pressing national security threats facing the United States.

It is important for the American people to understand the variety of nation-states and non-nation-state actors that remain serious concerns to our intelligence agencies and to the national security of the United States.

North Korea's threatening behavior towards the United States and our South Korean

allies continues at a high clip, even as their missile program makes rapid progress.

Iran's malign -- particularly malign -- and threatening behavior in the region and towards the United States threatens us in the region, our allies in the region. And I fear that Iran's nuclear program has advanced to a point where we would have little warning if they decided to produce weapons-grade enriched uranium and move on to the weaponization of that uranium.

Of course, Russia remains a central threat 1 year into Putin's brutal invasion of Ukraine. Last year, Chairman Turner and I had the opportunity to visit Kyiv and meet President Zelenskyy and his leadership to see firsthand the courage of the Ukrainian people who are defending their homeland. The assistance and support we have provided, along with our allies, have frustrated Putin's ambitions, but we have, clearly, a long way to go and some thinking to do about how to make sure that that conflict doesn't continue being the meat-grinder that it is.

Which brings me to China, which is the central, I believe, strategic challenge we face in the world, one marked by a complicated and interdependent economic relationship.

Last week, we held a hearing with leaders from the foreign policy community, and Dr. Richard Haass, most recently of the Council on Foreign Relations, observed that how ever one might characterize our relationship with China, the easy Cold War analogies to the Soviet Union are inapt. The Soviet Union was not integrated into the global economy.

For all our discussion of decoupling, the United States and China set a new record in 2022 on two-way trade between our countries, totaling \$700 billion. China currently holds close to a trillion dollars of United States sovereign debt.

So how do we respond to an increasingly aggressive and militaristic Chinese approach to world affairs? China clearly aspires to export its authoritarian approach to governance, including the technological tools that enable that regime to restrict speech and surveil their

people. How well do we know Chinese thinking, intentions, red lines, and weaknesses? As the policymakers navigate this difficult path, that will be an essential task for the Intelligence Community.

A word on technology, which I think I have talked to all of you about: For the first time since the Manhattan Project in the late 1940s, we are not the clear technological leader. Innovation is happening elsewhere. And, of course, innovation is happening at a rapid clip inside China.

And we no longer live in the era of planes and tanks and battleships. Technology today means artificial intelligence, quantum computing, and biosynthesis. None of those are areas in which we want to be even a fast follower. We want to be at the point of the spear on innovation on those things.

I concur with the chairman on 702. The people sitting here today understand that 702 authorities must be reauthorized. 702, unlike the Section 215 metadata collection program, is a 24/7, day-by-day, essential tool to keeping this country safe.

But the chairman is not wrong. The Congress -- we have a long way to go to educating the Congress on precisely what those authorities are.

I would note that many of the abuses that the chairman made reference to, or misbehavior, occurred not under FISA 702 but under other FISA authorities. And I note that just because we have a long way to go in educating the Congress of the United States and the people of the United States about exactly what it is that we are talking about.

And you have a long way to go to validating my statement that this is a 24/7, day-by-day, essential tool to keeping the American people safe.

So I look forward to our conversation, concur in the chairman's view that we are committed to pursuing the important work of this committee in a bipartisan, thoughtful, and constructive way, and welcome you again to testimony here today.

The Chairman. Thank you, Congressman Himes.

We now turn to Avril Haines, Director of National Intelligence, who will be presenting the opening statement on behalf of the panel.

Welcome, and thank you for your leadership, Director Haines.



**STATEMENT OF THE HONORABLE AVRIL HAINES, DIRECTOR OF  
NATIONAL INTELLIGENCE; ACCOMPANIED BY  
LIEUTENANT GENERAL SCOTT BERRIER, DIRECTOR OF THE DEFENSE  
INTELLIGENCE AGENCY; THE HONORABLE WILLIAM BURNS, DIRECTOR  
OF THE CENTRAL INTELLIGENCE AGENCY; GENERAL PAUL NAKASONE,  
DIRECTOR OF THE NATIONAL SECURITY AGENCY; AND THE HONORABLE  
CHRISTOPHER WRAY, DIRECTOR OF THE FEDERAL BUREAU OF  
INVESTIGATION**

Director Haines. Thank you very much. Thank you, Chairman Turner, Ranking Member Himes, members of the committee. Thank you for the opportunity to be here today, alongside my wonderful colleagues and on behalf of the extraordinary public servants we lead in the Intelligence Community, to present the IC's Annual Threat Assessment.

And before I start, I just want to publicly thank the men and women of the Intelligence Community whose work we are presenting today. From the collector to the analyst and everybody in between who made it possible for us to bring you the Annual Threat Assessment in hopes that this work will help keep our country safe and prosperous, thank you.

This year's assessment notes that, during the coming year, the United States and its allies will face an international security environment that is dominated by two sets of strategic challenges that intersect with each other and existing trends to intensify their national security implications.

First, great powers rising, regional powers, and an evolving array of non-state actors are vying for influence and impact in the international system, including over the standards

and rules that will shape the global order for decades to come.

The next few years are critical, as strategic competition with China and Russia intensifies and, in particular, over how the world will evolve and whether the rise of authoritarianism can be checked and reversed. How well we stay ahead of and manage this competition will be fundamental to our success in navigating everything else.

Second, challenges that transcend borders, including climate change, human and health security, and economic needs made worse by energy and food security, as well as Russia's unprovoked and illegal invasion of Ukraine, are converging as the planet emerges from the COVID-19 pandemic and all at the same time as great powers are challenging longstanding norms for transnational cooperation.

Further compounding this dynamic is the impact that rapidly emerging technologies -- Ranking Member Himes noted -- are having on governments, business, society, and intelligence around the world.

And given that background, the People's Republic of China, which is increasingly challenging the United States economically, technologically, politically, and militarily around the world, remains our unparalleled priority.

The Chinese Communist Party, or CCP, under President Xi Jinping, will continue efforts to achieve Xi's vision of making China the preeminent power in East Asia and a major power on the world stage.

The CCP is increasingly convinced that it can only fulfill Xi's vision at the expense of U.S. power and influence and by using coordinated, whole-of-government tools to demonstrate strength and compel neighbors to acquiesce to its preferences, including its land, sea, and air claims in the region and its assertions of sovereignty over Taiwan.

Last October, President Xi secured his third 5-year term as China's leader of the 20th Party Congress. And, as we meet today, China's national legislature is in session, formally

appointing Xi and confirming his choice to lead the PRC State Council as well as its ministries and the leaders of the military, legislative, and judicial branches. And after more than a decade serving as China's top leader, Xi's control over key levers of power give him significant influence over most issues.

Xi has surrounded himself with like-minded loyalists at the apex of the Party Standing Committee, China's highest decision-making body. And we assess that during the course of Xi's third term, they will, together, attempt to press Taiwan on unification; undercut U.S. influence, which they perceive as a threat; drive wedges between Washington and its allies and partners; and promote certain norms that favor China's authoritarian system.

And you may have seen Xi's recent criticism during his speech on Monday of what he referred to as America's suppression of China, reflecting his longstanding distrust of U.S. goals and his apparent belief that the United States seeks to contain China.

Xi's speech was the most public and direct criticism that we have seen from him to date and probably reflects growing pessimism in Beijing about China's relationship with the United States as well as Xi's growing worries about the trajectory of China's economic development and indigenous technology innovation -- challenges that he now blames on the United States. He also wants to message his populace and regional actors that the U.S. bears responsibility for any coming increase in tensions.

And despite public and directly critical rhetoric, however, we assess that Beijing still believes it benefits most by preventing a spiraling of tensions and by preserving stability in its relationship with the United States.

Specifically, Beijing wants to preserve stability in East Asia, avoid triggering additional economic punishments from U.S. sanctions and U.S. partners, and showcase a steady relationship with the United States to avoid setbacks in its other relationships around the world, even while signaling opposition to claimed U.S. provocations, including the

shoot-down of the PRC balloon. He wants a period of relative calm to give China the time and stability it needs to address domestic difficulties.

Xi's principal focus is on domestic economic development, which is not assured. The IC assesses that China's long-term economic growth will continue to decelerate, because China's era of rapid catch-up growth is ending and structural issues, such as debt, demographics, inequality, overreliance on investment, and suppressed consumption, remain.

And although the CCP may find ways to overcome its structural challenges over the long term, in the short term, the CCP continues to take an increasingly aggressive approach to external affairs, pursuing the goal of building a world-class military; expanding its nuclear arsenal; pursuing counter-space weapons capable of targeting U.S. and allied satellites; forcing foreign companies and coercing foreign countries to allow the transfer of technology and intellectual property in order to boost its indigenous capabilities; continuing to increase global supply-chain dependencies on China, with the aim of using such dependencies to threaten and cut off foreign countries during a crisis; expanding its cyber pursuits and increasing the threat of aggressive cyber operations against the U.S. homeland and foreign partners; and expanding influence operations, including through the export of digital repression technologies.

The CCP will also seek to reshape global governance in line with his preferences and governance standards that support its monopoly of power within China. Beijing is elevating PRC candidates and policies at the U.N.; attempting to gain buy-in for Xi's development and global initiatives; promote blocs like the Shanghai Cooperation Organization as a counterweight to the West; and shape multilateral groupings such as the formerly "17+1" forum in Eastern Europe, but with mixed success.

In brief, the CCP represents both the leading and most consequential threat to U.S. national security and leadership globally. And its intelligence-specific ambitions and

capability make it our most serious and consequential intelligence rival.

During the past year, the threat has been additionally complicated by a deepening collaboration with Russia, which also remains an area of intense focus for the Intelligence Community.

And when we were here last before the committee for the ATA, Annual Threat Assessment, last year, it was only a few weeks after Russia's unprovoked and illegal invasion of Ukraine. Now we are over a year into the war, which is reshaping not only Russia's global relationships and strategic standing but also our own and strengthening our alliances and partnerships in ways that President Putin almost certainly did not anticipate, often precipitating the very events that he hoped to avoid, such as Sweden and Finland's petition to join NATO.

And on the battlefield, there is currently a grinding attritional war in which neither side has definitive military advantage, and the day-to-day fighting is over hundreds of meters, currently focused in Donetsk, as Russia tries to capture the remainder of the oblast.

The Russians are making incremental progress on Bakhmut, which is not a particularly strategic objective, but are otherwise facing considerable constraints, including personnel and ammunition shortages, dysfunction within the military's leadership, exhaustion and morale challenges.

And even as the Russian offensive continues, they are experiencing high casualty rates. Putin is likely better understanding the limits of what his military is capable of achieving and appears to be focused on more modest military objectives for now.

Export controls and sanctions are hampering Russia's war effort, particularly by restricting access to foreign components necessary to produce weapons systems. And if Russia does not initiate a mobilization, a mandatory one, and identify substantial third-party ammunition supplies, it will be increasingly challenging for them to sustain even the current

level of offensive operations in the coming months. And, consequently, they may fully shift to holding and defending the territories they occupy.

In short, we do not foresee the Russian military recovering enough this year to make major territorial gains. But Putin most likely calculates that time is on his side, and prolonging the war, including with potential pauses in the fighting, may be his best remaining pathway to eventually securing Russia's strategic interests in Ukraine, even if it takes several years.

And Ukraine, of course, also faces challenges. Ukraine's prospects for success in a major spring offensive will probably hinge on several factors. At present, the Ukrainian Armed Forces remain locked in a struggle to defend against Russian offenses across eastern Ukraine. And while these Russian assaults are costly for Russia, the extent to which Ukrainian forces are having to draw down their reserves and equipment, as well as suffer further casualties, will all likely factor into Ukraine's ability to go on the offensive later this spring.

The IC continues to monitor Putin's reactions and his nuclear saber-rattling. Our analysts assess that his current posturing is intended to deter the West from providing additional support to Ukraine as he weighs a further escalation of the conflict. And he probably still remains confident that Russia can eventually militarily defeat Ukraine and wants to prevent Western support from tipping the balance and forcing a conflict with NATO.

And, of course, the already-considerable human toll of the conflict is only increasing. In addition to the many tens of thousands of casualties suffered by the Russians and Ukrainian militaries, more than 8 million people have been forced to flee Ukraine since Russia invaded.

There is widespread reporting of atrocities committed by Russian forces, including deliberate strikes against nonmilitary targets, such as Ukraine's civilian population and

civilian infrastructure, particularly its energy facilities and electrical grid.

Russia and its proxy groups almost certainly are using so-called filtration operations to detain and forcibly deport tens of thousands of Ukrainian civilians to Russia. And the IC is engaged with other parts of the U.S. Government to document and hold Russia and Russian actors accountable for their actions.

The reaction to the invasion from countries around the world has been resolute, hurting Russia's reputation in the world and generating criticism at home. Moscow has suffered losses that will require years of rebuilding and leave it less capable of posing a conventional military threat to Europe and operating assertively in Eurasia and on the global stage. And, as a result, Russia will become even more reliant on asymmetric options such as nuclear, cyber, and space capabilities and on China.

Our assessment also covers Iran, which continues to pursue its longstanding ambitions for regional leadership and is a threat to U.S. persons directly and via proxy attacks. Iran also remains a threat to Israel, both directly and indirectly through its support of Lebanese Hezbollah and other proxies.

And, most concerning, Iran has accelerated the expansion of its nuclear program, stating that it is no longer constrained by any JCPOA limits and has undertaken research and development activities that would bring it closer to producing the fissile material for completing a nuclear device, following a decision to do so.

North Korea similarly remains a proliferation concern, as it continues its efforts to steadily expand and enhance its nuclear and conventional capabilities, targeting the United States and our allies, periodically using aggressive and potentially destabilizing actions to reshape the regional stability environment in its favor and to reinforce its status as a de facto nuclear power.

In addition, regional challenges, such as interstate conflicts, instability, and poor

governance developments, also pose growing challenges. In Africa and the developing world, increased poverty, hindered economic growth, and widespread inequality are creating the conditions that are feeding domestic unrest, insurgencies, democratic backsliding, authoritarianism, and cross-border conflict spillover.

And several parts of the Middle East will remain plagued by war, insurgencies, and corruption.

In the Western Hemisphere, persisting economic weakness, insecurity, corruption are fueling public frustration and anti-status-quo pressures that very likely will present governance challenges to leaders while also posing sustained spillover migration, criminal, and economic challenges for the United States.

Throughout the world, countries are struggling to maintain democratic systems and prevent the rise of authoritarians, in some cases because Russia and China are helping autocrats take or hold power.

And as I noted at the outset, transnational challenges interact with more traditional threats and often reinforce each other, creating compounding and cascading risks to U.S. national security.

For example, climate change remains an urgent threat that will increasingly exacerbate risks to U.S. national security as the physical impacts increase and geopolitical tensions mount over the global response to the challenge.

And now entering its fourth year, the COVID-19 pandemic remains one of the most significant threats to global public health, at a cost of more than 6.5 million lives and trillions of dollars in lost economic output to date.

In addition to direct effects of the pandemic, resultant economic, human security, political, and national security implications of COVID-19 continue to strain recovery efforts, presenting both known and unforeseen challenges that probably will ripple through society



and the global economy during the next year and for years to come.

Russia's aggression against Ukraine has aggravated COVID-19-related fragilities in the global economy, raised commodity prices, fueled market volatility, and contributed to food insecurity and financial instability.

And the combination of elevated energy and food prices has increased the number of individuals facing extreme poverty and food insecurity. Affected countries will struggle to reverse these trends through 2023, even if global food prices stabilize.

And Russia's war in Ukraine can be blamed for these intensifying effects -- something much of the world also understands and that others, including China, will have to come to terms with as they consider to what extent they want to consider assisting or enabling Russia.

And climate change, the pandemic, and conflicts are exacerbating irregular migration. And in the Western Hemisphere, push and pull factors that drive migrants to the United States, such as deteriorating socioeconomic and security conditions, misperceptions of U.S. policies, and employment opportunities in the United States, will almost certainly persist through 2023.

And please forgive me, because apparently the last two pages of mine did not print out on this, so I am just going to grab my extra copy.

Okay.

Transnational criminal organizations exploit migrants through extortion, kidnapping, and human trafficking, including sex trafficking and forced labor. And these organizations also continue to pose a direct threat through the production and trafficking of lethal illicit drugs, massive theft, financial and cyber crimes, money laundering, and eroding the rule of law in partner nations.

In particular, the threat from illicit drugs is at historic levels, with the robust supply of synthetic opioids from Mexican TCOs continuing to play a role in driving American

overdoses to over 100,000 annually.

And terrorism, of course, remains a persistent threat, but the problem is evolving. Individuals and cells adhering to ideologies espoused by ISIS, al-Qa'ida, and transnational racially and ethnically motivated violent extremist movements, in particular, pose serious threats to U.S. persons, facilities, and interests.

And then two indirect threats that I think are worth highlighting:

New technologies, particularly in the fields of artificial intelligence and biotechnology, are being developed and proliferating faster than companies and governments are able to shape norms governing their use, protect privacy challenges associated with them, and prevent dangerous outcomes that they can trigger.

The convergence of emerging technologies is likely to create breakthroughs that are not as predictable and that risk a rapid development of more interconnected, asymmetric threats to U.S. interests.

Relatedly, foreign states' malicious use of digital information and communication technologies will become more pervasive, automated, targeted, and complex during the next few years, threatening to distort publicly available information and probably outpacing efforts to protect digital freedoms and, at the same time, educate audiences on how to distinguish fact from propaganda.

Authoritarian governments usually are the principal offenders of digital repression. And, of course, democracies, with open information environments, are the most vulnerable.

In closing, I want to bring to your attention the absolutely crucial authority that both Chairman Turner and Ranking Member Himes discussed will expire at the end of the year if Congress does not act, which is 702 of the Foreign Intelligence Surveillance Act.

I can tell you without hesitation that Section 702 was relied upon in gathering intelligence that was relevant to putting together this assessment, as it is hard to overestimate

the importance of this authority to our work every day. FISA Section 702 provides unique intelligence on foreign intelligence targets at a speed and reliability that we cannot replicate in any other authority.

Section 702 was originally enacted to enable the U.S. Government to quickly collect on the communications of terrorists located abroad. And the authority allows the IC to acquire foreign intelligence from non-U.S. people located outside of the United States who are using U.S. electronic communication service providers.

702 is still vital to our counterterrorism mission, as evidenced by its key role in the U.S. Government's operation against former al-Qa'ida leader Ayman al-Zawahiri.

But 702 is now principally relied upon for vital insights across a range of hard priority threats, including China, malicious cyber actors targeting U.S. critical infrastructure, weapons proliferation, attempting to evade sanctions to deliver precursor chemicals to hostile actors, and even key intelligence related to threats emanating from Russia, North Korea, Iran, and I will say China again.

I realize that Section 702 is a powerful authority, and it is incumbent on all of us in the Intelligence Community to ensure that the privacy and civil liberty interests of Americans are built into its design and implementation at every level. And over the last many years, we have significantly expanded oversight and dedicated resources to compliance in order to do just that. And we welcome the opportunity to work with you on reauthorizing this critical authority and building in your trust.

Thank you for your patience, and we look forward to your questions. Thank you.

[The statement of Director Haines follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

The Chairman. Well, Director Haines, it was incredibly impressive to watch you continue to read your statement while looking through your file. I don't know that any of us would have been able to do that, but Director Burns for the win. That was great.

Director Haines. As always.

The Chairman. Yeah. Excellent.

We will now begin with member questions, and I yield my time to Representative Darin LaHood, the chair of our FISA 702 working group.

Darin?

Mr. LaHood. Well, thank you, Chairman Turner.

And I want to thank the panel here today for your service to our country, and thank you for the work you do every day to keep our citizens safe and our country secure.

I am honored to be selected as the lead for this important working group on FISA reforms, and I am excited to take on the necessary review.

I concur with Chairman Turner that FISA, and specifically the authorities in Section 702, provide our Intelligence Community with an invaluable and irreplaceable tool that supports our national security apparatus in the fight against our foreign adversaries.

As a former assistant U.S. attorney and specifically as a chief terrorism prosecutor overseeing the investigations and criminal prosecutions of terrorist activities, I fully understand the value of FISA as an incredible collection asset in our fight against ongoing global and terrorist threats.

This committee has been briefed countless times on the many successes directly attributable to our 702 collection authorities, some of which, Director Haines, you highlighted in your opening remarks.

And I would also comment, I know, General Nakasone, last month, or I guess in

January, you spoke to the Privacy and Civil Liberties Oversight Board on the value of 702. In that speech, you talked about, "This authority provides the U.S. Government with irreplaceable insights, whether we are reporting on cybersecurity threats, counterterrorism threats, or protecting U.S. and allied forces. FISA Section 702 has helped us understand the strategic intention of the foreign governments we are most interested in, including the PRC, Russia, Iran, and North Korea."

Unfortunately, there are far too many Members of Congress, on both sides of the aisle, that question whether the executive branch can be trusted with this powerful tool. And that is because, in the past and currently, there has been abuses and misuses of 702 by the FBI.

From where I sit today, I believe that a clean legislative reauthorization of 702 is a nonstarter. To reiterate what the chairman said, you must first acknowledge that a problem exists before we can formulate meaningful reforms to build back trust and confidence in the FISA process.

Director Wray, I want to start with you and ask, are you willing to acknowledge that the FBI has committed abuses and violations in its use of FISA, and is that defensible.

Mr. Wray. Well, first off, no violations are defensible, in my view.

It is important to distinguish, as I think both the ranking member and the chair may have, between things that happen with Title I FISA, you know, for example, that were at issue in the Inspector General report related to the Crossfire Hurricane matter -- which, as I have said before, describes conduct that I consider totally unacceptable, totally unacceptable, and unrepresentative of the FBI. And we implemented all sorts of reforms that I could go into on that.

Then, over on the 702 side, there have been compliance incidents that have to be addressed. And we have taken all sorts of steps that I could walk the committee through

here to address that issue.

And what is important to note about that is that all of the reports to date that have been shared with the public and I think with the Congress about 702 compliance issues all predate -- that is, the conduct at issue predate all these reforms.

Which is why it is so important for me to be able to let the committee know -- and this will be coming in more detail in the next ODNI report that comes out in late April, I think it is -- that we have now seen a 93-percent decrease year over year, from 2021 to 2022, in the number of U.S.-person queries made by, you know, the FBI.

And that is not just an aberration of that 1 year. If you compare it to 2020, so the year before that, it is about an 85-percent increase. So it is a dramatic increase in the judiciousness with which our people are running their queries.

And we are absolutely committed to making sure that we show you, the rest of the Members of Congress, and the American people that we are worthy of these incredibly valuable authorities.

Mr. LaHood. Well, I appreciate you mention that.

I would say, because of a number of these abuses and non-compliance issues with the FBI, would you agree that the FBI has a trust issue with the American public and specifically with Members of Congress?

Mr. Wray. Well, certainly, any time we have anybody who has a trust issue with us, we want to try to address it.

I think, when I look at the American people more broadly, I think a lot of it is reaction to specific cases here and there, but I will tell you that I see the American people showing up in droves to come work at the FBI.

Putting that to the side -- putting that to the side, we clearly have work to do, and we are eager to do it with this committee, to show that we can be worthy stewards of these

important authorities.

And so, if there are questions that need to be answered, I understand completely why those questions are being raised. We brought them on ourselves. And I want to make sure that we can show you that we can answer those questions.

Mr. LaHood. And how do you give reassurance to the American people that their civil liberties are going to be protected?

Mr. Wray. Well, the changes that I started describing at a high level include all sorts of things. So that is everything from system changes that prevent even -- even -- inadvertent compliance incidents, that is new safeguards, new approvals, new oversight, all sorts of mandatory enhanced training.

I created and stood up an entire new Office of Internal Audit that did not exist at the FBI before and brought in a former agent who is also a former Big Four accounting firm partner to run that Office of Internal Audit. And that office is focused exclusively on FISA compliance.

Ultimately, in the long run, we want that office to take on other kinds of compliance too, but because of the importance of this issue, because of the importance of the concerns that you and others have framed, we have dedicated that Office of Internal Audit to focus exclusively on this important authority and compliance with it.

So those are some of the things. Obviously there is a lot more that I could get into, but I am sympathetic to the time constraints here.

Mr. LaHood. Well, thank you for that.

Unfortunately, I believe that the FBI does have a significant trust issue with Members of Congress. And that is part of what we will deal with with the working group.

And I would say that trust has only been made worse by the recently declassified Section 702 Compliance Report covering December 2019 through May of 2020. In that

report, there was a number of concerning things that were brought forward. There were queries done inappropriately by the FBI on a local political party.

And then, secondarily, included in there was one specific instance of abuse involving multiple queries of a sitting Member of Congress in the FBI's FISA databases. Buried in a footnote of the declassified assessment, this specific instance is described as follows:

Quote, "An intelligence analyst with the FBI conducted multiple queries using only the name of a U.S. Congressman. The 707 report describes the specific facts that led the analyst to conduct these queries. These queries retrieved unminimized FISA-acquired information, including Section 702-acquired products that were opened. FBI advised that no minimized FISA-acquired information was disseminated or used in any way."

This was reviewed, obviously, by the National Security Division of the U.S. Department of Justice and ODNI. And, based on what they reviewed, they found these queries to be wholly inappropriate, not compliant, and a violation, because they were overly broad as constructed.

I think that the report's characterization of this FBI analyst's action as a mere misunderstanding of querying procedures is indicative of the culture that the FBI has come to expect and even tolerate.

It is also indicative of the FBI's continued failure to appreciate how the misuse of this authority is seen on Capitol Hill. And I want to make clear, the FBI's inappropriate querying of a duly elected Member of Congress is egregious and a violation not only that degrades the trust in FISA but is viewed as a threat to the separation of powers.

I have had the opportunity to review the classified summary of this violation, and it is my opinion that the Member of Congress that was wrongfully queried multiple times solely by his name was, in fact, me.

Now, this careless abuse of this critical tool by the FBI is unfortunate. Ironically, I



think it gives me a good opportunity and a unique perspective on what is wrong with the FBI and the problems that the FBI has.

To highlight that, I would like to submit for the record a couple things.

February 28th, 2023, Director Haines and Attorney General Garland asked for a reauthorization from the Congress, but they go on to add that there needs to be rigorous and ongoing oversight of the FBI's 702 querying, specifically their collection decisions on U.S.-person inquiries, and they will be evaluating and taking remedial action to address identified incidents of noncompliance by the FBI.

I would like to submit that for the record, Mr. Chairman.

The Chairman. Without objection.

[The information follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

Mr. LaHood. Secondly, a letter was sent to you on February 15th, Director Wray, 2023, from Congressman Andy Biggs of Arizona, and he talks about the declassified 2021 report detailing these continued abuses of 702.

In there, he mentions that these instances should frighten every American, and Congress deserves an explanation for them. He additionally talks about, these, quote, "backdoor" searches are a violation of the Fourth Amendment and cannot continue.

I would ask to submit that for the record.

The Chairman. Without objection.

[The information follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

Mr. LaHood. Thirdly, article in Politico from March 1st, titled "DOJ Faces Bipartisan Phalanx or Army of Skeptics on FISA 702."

In that article, again referring to this declassified report on the inappropriate use of 702, it talks about -- I will quote here: "In a sign of odd political bedfellows in the House who are pushing reforms, conservative Congressman Andy Biggs and progressive Member Pramila Jayapal, both members of the Judiciary Committee, publicly vented on the detail tucked in the footnote of the report: An FBI intelligence analyst improperly queried surveillance data on a U.S. Member of the House."

I would ask to submit that for the record.

The Chairman. Without objection.

[The information follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

Mr. LaHood. Lastly, the footnote that I mentioned that has been declassified states in there that "the National Security Division of the U.S. Department of Justice and ODNI assessed, based on the facts and analysis of this FBI analyst, that these queries were not compliant because they were overly broad as constructed."

I would like to submit that for the record.

The Chairman. Without objection.

[The information follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

Mr. LaHood. The bottom line is, 702 deserves to be reauthorized because it is an invaluable tool to our efforts to counter the threats of our adversaries, but the FISA working group must and will pursue reforms and safeguards through this reauthorization process.

To help explain to the public why 702 should be reauthorized, I have a few questions for our other panelists.

Director Haines, why do we need 702 to specifically counter China?

Director Haines. Thank you, Representative.

Specifically with respect to China, there are a number of ways in which 702 is crucial.

It is crucial in the context of counterintelligence, where we are looking at where it is that China's efforts to send spies into the United States may be and what their planning is in relation to it.

It is crucial in the context of threats to, you know, U.S. victims and to critical infrastructure through cyber.

As we have all indicated, it is crucial to understanding a whole range of issues, because it is effectively the most, sort of, effective way for us to gather intelligence against non-U.S. persons outside of the United States.

Mr. LaHood. Thank you.

And, Director Burns, what does 702 mean for the CIA's ability to counter China?

Mr. Burns. It is crucially important for all the reasons, sir, that Director Haines just mentioned.

It also enables us to focus on efforts to evade sanctions, to steal intellectual property, to obtain sensitive technologies as well.

And so, in all those areas, it is extremely important.

Mr. LaHood. And, Director Nakasone, can you quantify in some way how vital 702

is to the NSA's efforts to counter China? And I know you specifically referenced a number of incidents in your speech in January.

General Nakasone. I would quantify it, Congressman, by saying, it is the number-one authority that we need.

I can go into closed session with regards to the specific areas where it is so important.

Mr. LaHood. Thank you.

And, Director Berrier, as a consumer of the information obtained by 702, can you explain the value of this information in DNI's efforts to counter China.

General Berrier. Yes, I can. As an all-source intelligence agency, while we don't do FISA collection, we certainly benefit from the insights we get from that. We bake that into our all-source analysis to eliminate threats for the Department of Defense and the Nation.

Mr. LaHood. Thank you for that.

In closing, I am honored by Chairman Turner's selection as the chair of the FISA working group, and I am energized to begin our bipartisan work with the Judiciary Committee and our Senate colleagues to reform and reauthorize this vital tool.

I also look forward to working with all of you here before us today and request your cooperation in this endeavor.

Thank you, and I yield back, Mr. Chairman.

The Chairman. Ranking Member Himes?

Mr. Himes. Thank you, Mr. Chairman.

And thank you again to our witnesses.

My good friend from Illinois put a lot on the table there, much of which, unfortunately, I was not briefed on.

So, Director Wray, I would love to start just by giving you a minute or two to respond if you would like. But I would like you to keep it to a minute or two, if you would.

Mr. Wray. Obviously, there is a lot to say, so I will be very brief.

I completely understand Congressman LaHood's concerns and everything he read.

The main point I would make for today's purposes is that all of those problems -- and they are problems -- all of those compliance violations -- and they are violations -- predate -- predate -- all of these reforms that I was trying to summarize.

And so my hope is that we will be able to show, by working with the working group, how these reforms will prevent stuff like what you described from happening again in the future.

Mr. Himes. Thank you, Director Wray.

I am going to direct my next question to Director Haines and Director Burns.

We spend a lot of time thinking about the mechanics and tactics of what conflict with China would look like, and we don't spend a lot of time thinking about the economics of tension leading to, ultimately, conflict, were that to occur.

This is not current, but RAND did a study in which they estimated that Chinese GDP, in the event of a conflict, would contract by a staggering 25 to 35 percent. U.S. GDP could contract by 5 to 10 percent if there was conflict in the Taiwan Strait.

So the perplexing thing here is, this is a country that, really, the sole reason that it has been able to achieve the economic growth that it has, to the point where today it is, on an aggregate basis, the largest economy in the world, has been engagement with the world -- licit engagement through trade and other things and illicit engagement through the stealing of IP, the manipulation of currency rates over time, et cetera.

So I wonder -- two-part question -- can you paint a picture of, if tensions continue to be exacerbated, leading to a point where there is conflict, what that would look like for the global economy, for the Chinese economy? And, most importantly, help me understand why a Chinese leader would risk the golden goose, essentially.

Director Haines. I will start.

So I think, to your point, Representative, it is not our assessment that China wants to go to war. And that is something, I think, to start with. In other words, they are -- you know, we continue to assess that, for example, even with respect to Taiwan, that they would prefer to achieve unification through peaceful means as opposed to through a use of force.

They nevertheless are utterly committed to unification. And I think that is the challenge. In other words, Xi has made it quite clear that that is something that has to happen. And, as a consequence, if they believe that peaceful unification is not an option, then they are in the potential for actually trying to achieve it militarily, and they are certainly planning for that potential.

And then in terms of the impact that it would have, I think, you know, obviously it depends on what the conflict looks like. But, to your point again, I think it is absolutely right that this is -- any conflict is likely to have enormous economic implications.

And one of the things that we have certainly looked at and that others, you know, within the government -- Treasury and Commerce and so on -- have looked at is the implications with respect to Taiwan of a disruption of, you know, their materials, particularly their semiconductors.

And, you know, studies show that it would actually have absolutely enormous implications for the global financial economy if there were disruption to Taiwan's semiconductor production. Because, really, you know, the semiconductors, the chips that come out of Taiwan are present in virtually every category of electronic devices around the world.

I will leave it at that.

Mr. Himes. Director, I know CIA conducts economic work and economic assessments, so I would be interested in your view.



Mr. Burns. Sure. And I would just add two examples to what Director Haines said in terms of the calculus of the Chinese leadership, both on Taiwan and in terms of its relationship with Russia.

I think on Taiwan, while, as Director Haines said, we don't see evidence today that Xi has made a decision to invade Taiwan, I would never underestimate the ambitions of the current Chinese leadership in that regard or their determination.

I do think that nobody has watched more intently Vladimir Putin's experience in Ukraine than Xi Jinping has. And I think he has been sobered, to some extent -- at least it is our analysis -- by the extent to which the West was able to maintain solidarity and absorb some short-term economic costs in the interest of imposing even greater long-term economic costs on Russia.

That is something that President Xi has to weigh as he comes out of Zero COVID, tries to restore Chinese economic growth, tries to engage with, you know, the rest of the global economy.

And I think that also, you know, weighs in his decision about whether or not to supply lethal equipment to Russia. We see clear evidence that the Chinese leadership is considering that, not that it has made a decision, not that it has begun lethal shipments. But there again, I think that economic factor, as Director Haines said, has to weigh significantly in the calculus of the Chinese leadership.

Mr. Himes. Do we believe that the Chinese leadership sufficiently appreciates -- even were they to supply lethal weapons, that would have economic consequences. An awful lot of people around the world would be much more hesitant to do business with China.

Do we believe that the leadership in Beijing understands how that is a first step towards, again, killing the golden goose that has allowed that country to grow economically?

Mr. Burns. I think the only thing that I would highlight, Congressman, is that I think it has been important that European leaders have spoken up on this issue as well. Because I think, for a long time, the Chinese leadership has assumed that it could drive wedges between the United States and our European allies on an issue like this. I think the fact that several prominent European leaders have spoken out directly about this is a very important step.

Mr. Himes. Thank you.

Second category of questions is on technology. And I want to be respectful of my colleagues' time, so I am going to direct the questions to General Nakasone and General Berrier.

I had the opportunity last week to visit CIA and see the work that has been done by the Director in terms of technological innovation. Director Burns has made it a strategic priority. He hired somebody from the outside to be Chief Technology Officer.

The visit was amazing. This new Chief Technology Officer cleared out offices, created an open floor space. There are free snacks. They are just, you know, missing a millennial playing the guitar to reproduce what you see in Palo Alto every day in the middle of CIA headquarters.

So, with that as context, what are you guys doing -- I will start with you, General Nakasone -- what are you guys doing that is as tangible as what CIA has done to make sure that we are at the cutting edge of technological innovation?

General Nakasone. One of the things we have done, Ranking Member, is look at different partners. This is the key piece of what we have learned from Russia-Ukraine. The private sector been incredibly helpful in terms of where we need to go in being able to thwart what Russia has attempted to do in Ukraine.

We have opened up a cyberspace collaboration center, an unclassified building where our analysts go to engage with the private sector and members of the defense industrial base

to do two things: One is to provide information to the defense industrial base in terms of what is going on in the domain of cyberspace. Two is to also get information from what we are seeing out there. What are the new leads? What are the things that we have to be able to emphasize?

The coming decade is certainly a decade where cyberspace will be dominant. One of the things that we believe is that we have to have those partnerships that are so critical.

Mr. Himes. General Berrier?

General Berrier. Congressman, our innovation engine is really fueled by this thing called NeedipeDIA. This is where companies can come in with great ideas on how they might be able to help the defense intelligence enterprise. We evaluate those ideas, we meet with those folks, and then we try to pull their ideas in.

Our two major focus areas right now are AI and ML for our program called MARS, the Machine-Assisted Analytic Rapid-Repository System, which will revolutionize the way we do foundational military intelligence, really pulling in swaths of data to make that environment much richer for our analysts.

And the other piece is really our MASINT sensor modernization, to be able to take all of those varieties of signals that are out there that are new and unique and be able to pull them into our MASINT enterprise. That is a focus of DIA.

Mr. Himes. Thank you, General Berrier. I appreciate that.

And I am glad you highlighted openness to outside companies that are not the traditional primes. I think that only gets you about a third of the way there, because I have just heard too many stories of innovative companies who just have no hope of navigating the acquisition process and authorities and everything else, even though they may have cutting-edge technology far better than what would be -- so I am going to follow up with you on that and yield back my time.

Thank you, Mr. Chairman.

The Chairman. Thank you.

Dr. Wenstrup?

Dr. Wenstrup. Well, thank you, Chairman Turner, Ranking Member Himes, and all of you for being here today.

Director Haines, you cut right to it today about the challenges that we face as a Nation, the threats that we have. The threats to our country are not new, but some of the forms of those threats are new. And I want to talk about that a little bit.

The Chinese Communist Party is very assertive. They want to destabilize us as much as they can, and they are getting pretty good at it.

So the growing concerns I have are -- the development of adversaries' biological weapons is of grave concern to me and also the flow of illicit fentanyl coming into our country, which, even in a meeting with the Chinese Ambassador, he admitted, "We sell the precursors. Those are legal products. You know, it is somebody else's problem after that."

Well, it is our problem. And I do want those accountable for these efforts to be held accountable at some point, and we have to do a better job of that. And I think we need to address and invest in the resources we need to stop the scourge of this fentanyl, illicit fentanyl. And, also, the creation of bioweapons is something we should be greatly concerned about, as with any weapon an adversary may carry. So it is our responsibility, I think, to really work together on these things as best we can.

We had a panel a few weeks ago. Dr. Heather Wilson was there, and I asked how we could work together a little bit better, in her eyes. And she mentioned how the law requires members of this committee to be fully and currently informed of the intelligence activities of the United States.

That is this committee. It is not every Member of Congress. It is not the general

public. And we all get that. But for this committee, it has to happen. And we need to insist upon that.

And we also need to insist, on our side, that we engender trust to the seriousness of this committee and the work that we have to do and our own professional responsibilities in this relationship. And I think we are at that point -- I really do -- with this committee right now.

But we have the responsibility of oversight, as well as working with all of you. And, in my mind, there can be no walls between us. There can be walls around us at times. There needs to be walls around us at times. But there should be no walls between us if we are going to be effective. And we really can only move at the speed of trust.

And I feel like I have developed relationships with all of you. It has been very helpful to the work that we do on this committee, and I thank you for that. Sometimes we can do a little bit more.

And so, Director Haines, I know this committee has written you a few times about who the Intelligence Community consulted with regarding the assessment of COVID-19 and its origins.

Now, I chair the Select Subcommittee on the Pandemic, all things with the pandemic. And the origins of COVID is important. And even yesterday in our hearing, every person on the committee, bipartisan, and every one of our panelists said, finding the origins of COVID is an important project we need to continue and try to get to. And we could go into all those reasons.

You know, why is it important, though, for us to have this information and to know who the experts are? And, you know, if we hear something like, "It is our policy not to tell you on the committee who we spoke to," that is a problem. And it is important who you spoke to, because if who someone spoke to may have some personal bias or other agenda or

political bias towards their conclusions -- I mean, look, you have seen all these agencies with different conclusions. Well, why is that? Well, part of that may be depending upon who they talk to.

So that is important, that we get that information. And it is my understanding that DOE would be willing to show us their underlying report, especially -- or updated report, but since ODNI owns the assessment, you would have to approve that.

So what I am going to ask is that you would approve that and get us that information so that we can move forward. And I would hope that we can also get the information of actually who they talked to, because it is important to this committee, it is important to the country.

So I guess I am just asking, would you commit to that at this time?

[11:02 a.m.]

Director Haines. Thank you so much, Congressman.

I know this is an issue that we have talked about before --

Dr. Wenstrup. Right.

Director Haines. -- and I think, first of all, on the DOE assessment, absolutely. I suspect it we would have to be in classified forum. I am sure --

Dr. Wenstrup. Sure.

Director Haines. -- it is a classified report. But more than happy to share any final assessment that they have done. If they are comfortable with it, I can't imagine myself standing in the way. So I don't know what that is, but we will look into that and get back to you quickly.

I think, on the more general issue, let me just put a few things down.

I think one problem for us is that we obviously want to be able to consult with outside expertise, including academics, a variety of others experts in, you know, fields related to COVID-19 but also a series of other areas that we work in. And, often, for many academics that we consult with, it is not something they want to -- they do not want to be known as consulting with the Intelligence Community. It creates challenges for them and all those things --

Dr. Wenstrup. If I may, I am talking about in a classified setting.

Director Haines. No, no. I am --

Dr. Wenstrup. And --

Director Haines. So let me finish. I will just --

Dr. Wenstrup. And this is important -- and this is important to the work, because we do need to know who they are and how they came to their assessment.

Director Haines. Congressman, let me just finish.

Dr. Wenstrup. Okay.

Director Haines. I will explain.

Dr. Wenstrup. Sure.

Director Haines. So often what will happen is, they will, for example, be willing to participate in a conference or something along those lines that is not for us, and they will do it under Chatham House rules that says that we can't attribute, essentially, anything to them specifically, even though we can bring the information out. That is an example of the kind of challenge that we end up in.

So what we have been able and willing to provide, in classified or in unclassified -- and we have given this, obviously -- is basically the backgrounds of various experts that we have consulted with, the actually published information that we have relied on, and --

The Chairman. Director --

Director Haines. -- answer any questions --

The Chairman. Director --

Director Haines. -- about how we got to a --

The Chairman. Director, I am going to need you to conclude.

Director Haines. Got it.

And I will just finish with the last thing, which is that, if there is anybody, sir, that you want us to talk to that you feel like we haven't, I commit to you that we will absolutely take those names and we will ensure that we are consulting with them as well.

Dr. Wenstrup. We are just trying to do the best job we can to, in the future, be able to predict a pandemic, prepare for it, to protect the American lives, and to prevent one if we can.



The Chairman. Mr. Carson?

Mr. Carson. Thank you, Chairman and Ranking Member.

This is an open question: Last week, our committee heard from several respected leaders from the think-tank community. And, in their remarks, they presented differing views about whether a standalone, open-source agency is needed in the IC.

What are your views? And what are your agencies doing to incorporate open-source reporting in its analysis to help counter the threats described in your remarks?

Director Haines. I will just start, but I think going to Director Burns and to General Berrier would be useful for you to hear what they are doing, because they are really centers of excellence in this area.

We have been through a process whereby we have been trying to ensure that the open-source work that is being done across the community essentially is as effective as possible in supporting the priorities across the Intelligence Community.

And one of those issues that has come up is, how do we organize ourselves, how do we ensure we have the right talent, how do we ensure we are supporting the technology that is needed and maintaining the partnerships with the private sector and otherwise that are important to this effort?

And we had an external panel look at that, and we have received advice. And we are going to be establishing at ODNI an OSINT executive, which is a small group -- it will be, like, a dozen folks if we go forward with this -- basically to support the work that is being done across the Intelligence Community.

The CIA is the functional manager for us on OSINT, and the DIA is the Defense Intelligence Enterprise manager on this, so I will turn to them.

Mr. Burns. Sure.

No, just to add, Congressman, I mean, I take very seriously the increasingly important

role of open-source information. We can't function effectively as an intelligence service, as the functional manager across the Intelligence Community, unless we put more resources, more drive, more energy into this issue.

So I appointed a new director of our open-source enterprise several months ago, and I am really pleased with the drive and energy and creativity that he is bringing to this as well, not only to make better use of artificial intelligence and machine learning -- because the challenge for us, for our analysts, is sifting through, you know, the avalanche of information that is out there, sifting through the haystack to get to those needles that are going to matter most to human analysts, and doing it very quickly.

And then to work with Director Haines and General Berrier and our other partners in the IC to avoid duplication, so, you know, we are learning from one another's experiences, and then also, I think, to look at ways in which we can learn from one another on training, on governance issues as well.

So I am pleased with the progress we are making, but I am determined to continue to drive this.

General Berrier. Congressman, we think that open-source, when combined with other sources of information that are classified, really comprises the secret sauce for all-source analysis.

And so I would say, from a Defense portfolio side of the house, what we are trying to do is formally establish the Defense program so that we have standards for training, tradecraft, that we are not getting ripped off in multiple places by buying the same kind of data, and that we are doing this in a way that is smart across the services and across the combatant commands.

Mr. Carson. Lastly, Chairman, recently we heard from several speakers, including General Petraeus, who warned of a lack of a genuine workforce development training in the

IC.

What are your organizations doing to improve diversity when it comes to recruiting and retaining your workforces? And if you agree that the IC needs to devote more resources to professional development, how do you all plan on tackling those very apparent issues?

Director Haines. Yeah. Thank you very much, Congressman.

I think there is no question that we have to do better on diversity, equity, and inclusion and accessibility. And I think you will see in our budget requests, in our proposals, in all of the work that we are doing, that we see this as an area that we need to focus more intense resources and efforts.

I will tell you that, you know, as a general matter, when I look across ODNI, for example, in the senior leadership, you know, and I look at the percentage of Hispanic and Latinos, for example, it is, you know, a little bit more than 3 percent, and that clearly does not reflect the country.

These are things that we are trying to get out. So the first part, from my perspective, is ensuring that we have data that is reliable, that allows us to be held accountable to what our diversity, equity, and inclusion is, and that we are able to do barrier studies and work that allow us to understand where there are challenges.

We are also working across a range of other issues that we have seen to sort of promote recruitment across the country in a variety of different communities to ensure that we are reaching folks that don't normally come to the IC or know about the IC, that we are focused on retaining the diverse talent that we do have.

We have recently looked at a project that would help to promote --

The Chairman. Director, I am going to have to ask you to summarize.

Director Haines. Sorry.

The Chairman. In order to get through the list that we have -- and we are going to

have to close the list -- we are going to have to start keeping everyone to the 5 minutes.

So if you would make your answers just a little bit shorter so we can get to everybody and get to the closed session.

Director Haines. I will stop there and let everyone --

The Chairman. All right.

You yield?

Mr. Carson. Thank you, Chairman.

The Chairman. Thank you.

Mr. Stewart?

Mr. Stewart. All right. I am going to talk really fast then.

There are a couple things I do want to talk about, and, again, to hit them both, I am going to be very brief on the first one, and that is 702, to reemphasize the importance of that.

Thanks for all of you being here. We recognize that each of you are distinguished leaders.

If I could make this point in introduction to 702, all of us are responsible to the people, but those of us sitting up here have a special responsibility to the people. We go home every weekend, and we talk with hundreds of people. I think we have a pulse on where the people are, far more than the Executive, far more than military or intelligence officials, and, I would say, far more than the Senate.

And so I think we have a pulse of the people. And, in that regard, then, when we talk about 702 and the fear and concern they have -- Director Wray, if I could, I am going to read you a communication I had from a constituent who is a national security expert, official, and then I would ask you to respond, or maybe you don't want to.

But I read this to you to illustrate, this is the challenge we have when it comes to reauthorizing. And much of this is shared by Members of Congress as well.

But, quoting from him: "We could show dozens of examples -- sending FBI agents to shut down local prosecutors for going after Jeff Epstein; systemic abuse of FISA; systemic abuse of First Amendment rights; targeting parents and Catholics; refusing to investigate multiple reports of sexual abuse of U.S. gymnasts. The problem is," speaking of the FBI, "they have no accountability, near-absolute power, and they know no one, not even Congress, can touch them."

That is what many, many Americans feel.

And now we have to go to them to say, "Yeah, we understand your concerns, but, at the same time, we want to reauthorize these powers and authorities."

I read that for you, as we discussed earlier, as a challenge we have. You are welcome to respond to it, although please do so briefly, or if you just recognize, "Yeah, we need to admit to the American people that we have made mistakes, and we are going to correct it."

Mr. Wray. So, Congressman, I appreciate you sharing your constituent's letter with me.

What I would say is, of course, like any major institution, we have made mistakes. Some of the descriptions in the constituent's letter are not accurate, in terms of what actually happened, but, absolutely, we have made mistakes.

And, to me, the mark of a leading organization is not whether it makes mistakes or not -- all major organizations, all elite organizations do -- but whether or not we learn from those mistakes. And I think we have. We have made all sorts of changes, which I could go into, on different issues.

But we are determined to be worthy of all Americans' trust, including your constituents.

Mr. Stewart. Well, and I appreciate that, because that is where we are going to find success, is if we can say that we recognize that we can do better, and, to do better, the process

has got to be reformed somewhat. And we look forward to working with you, because we do have to reauthorize 702.

Director Haines, this is to you. I think you are probably most appropriate to answer this. I mean, there are so many things we could talk about here. We look forward to the closed hearing, as I said. But we have to talk about China.

I reflect back on my military experience. There were a number of incidents, you know, a couple times when we had American assets, American intelligence aircraft who were captured or had a forced landing in China. The P-3 incident with the J-8 is an example. And, during that time, we didn't really know what our policy would be, how the U.S. would respond.

In the past, the President has said pretty clearly that we would respond with military action if China were to invade Taiwan. And then, shortly after that, the administration kind of walked back those comments. But it didn't occur just once; it occurred several times.

We have this policy of strategic ambiguity, which has served us well for the last 30 years. But I wonder if it is not time for us to declare another policy, a new policy, and that is: We will defend Taiwan. It is pretty clear the President seems to think that.

And I think, if we are going to deter -- again, understanding the need for strategic ambiguity before, but times are different now. If we are going to deter, I think we have to be clear in saying, "Yes, we will defend Taiwan militarily if we have to."

Director, am I wrong? And has there been a change in the administration's policy regarding ambiguity?

Director Haines. Thank you, Congressman.

I am obviously not in a position to comment on policy, but I certainly -- I think you are right in recognizing the President's comments on this issue and that that has been a pretty strong statement.

Mr. Stewart. Okay.

So let me -- in the 13 seconds I have, do we agree that there would be stronger deterrence if our adversaries knew that we would defend militarily if necessary?

Director Haines. You mean sort of -- in this particular case, I think it is clear to the Chinese what our position is based on the President's comments.

Mr. Stewart. Thank you.

And I only went 10 seconds over, Mr. Chairman, so I yield back.

The Chairman. Very, very good.

Mr. Krishnamoorthi?

Mr. Krishnamoorthi. Great. Thank you, Mr. Chair.

And thank you, Mr. Himes, for unearthing evidence of free snacks at the NSA.

We will be visiting shortly, General Nakasone.

My first question is directed to Director Wray.

Mr. Wray, you have said that TikTok, the popular app on people's phones, is, quote, "a tool that is ultimately within the control of the Chinese Government, and it screams out with national security concerns," close quote.

We found that TikTok and ByteDance employees regularly engage in a practice called "heating," in quotes, "heating," a manual push that ensures specific videos, quote, "achieve a certain number of video views."

Mr. Wray, can you rule out that TikTok is heated content at the direction of the CCP?

Mr. Wray. I don't think we could rule that out.

Mr. Krishnamoorthi. Now, let me just talk about another instance of what I think is very problematic behavior at TikTok and ByteDance, their parent company.

In December of last year, ByteDance confirmed it used TikTok to monitor U.S. journalists' physical location using their IP addresses in an attempt to identify whether they

had been located by ByteDance employees.

Can you rule out that this data was also shared with the CCP?

Mr. Wray. I don't think we could rule that out.

Mr. Krishnamoorthi. Could the CCP use TikTok to shape political opinion, such as to misinform the American public?

Mr. Wray. What you just described there is one of the concerns that we have -- namely, that the control of the recommendation algorithm could be used to conduct influence operations.

And, much along the lines of your first two questions, it is important to understand that that is not something that would be easily detected or ruled out, as you say. And that is just one of the several security concerns that we have about TikTok.

Mr. Krishnamoorthi. Thank you.

Director Haines, recently my staff described to me a term called "guanxi." Apparently, "guanxi" is a Chinese term that refers to a part of Chinese culture where people develop a personal trust and a strong relationship that can involve moral obligations in exchange of favors. And they suggested -- in the press, there had been suggestions that guanxi has developed between Chairman Xi and Vladimir Putin.

Let me ask you this question: Do we have any evidence that, in Chairman Xi's calculations of potentially providing military assistance to Russia in Ukraine, that he has ever discussed or he has discussed among his internal cadres potential assistance by Russia to China and the PRC in a potential invasion of Taiwan?

Director Haines. Thank you, Congressman. I think maybe we could discuss this in closed session.

Mr. Krishnamoorthi. Okay. Very good.

General Berrier, I want to talk to you about something called "peace disease," which



Chairman Xi has talked about repeatedly in his speeches recently.

This is what a former general of the Central Military Commission in the PRC has described as "peace disease." He said, quote, "Today, the PLA hasn't been in actual combat for many years, yet the fires of war are burning throughout the world. In this area, the gap between the PLA and foreign militaries is growing day by day." And then he closes with the quote, "This is an actual problem," close quote.

This was a quote from a 2009 speech by the general of the Shenyang Military Region.

This term, "peace disease," that refers to supposedly a lack of combat readiness on the part of the PLA has appeared 565 times in the PLA Daily between 2012 and mid-2018. And, just recently, Xi Jinping said he wants to cure the peace disease.

How do you assess when Chairman Xi would know that the peacetime disease has been cured and that their troops are ready for combat?

General Berrier. I am not sure that we could actually put a fixed date on that. We know there are a few dates out there, like 2027, 2035, and 2049. And we know that his leaders don't have the kind of combat experience that, say, the American military leaders have.

So we think that this is in his mind and perhaps shapes the way that he thinks about the readiness of his force. And we could probably go into a few more details on that in a closed session.

Mr. Krishnamoorthi. Very good.

Director Burns, I wanted to ask you a question about threats from ChatGPT, but I just couldn't think of any. So I went to ChatGPT, and I said, "Ask a question of CIA Director Burns about threats from ChatGPT."

It said, "Director Burns, what measures is the CIA taking to monitor and mitigate potential risks associated with the use of AI language models like ChatGPT? And how

would you prevent AI language models not to be used by malicious actors to spread false information or influence public opinion?"

That is from my pal, ChatGPT.

Mr. Burns. Sure. I am glad to give you an example, which I am sure ChatGPT is very well aware of, and that is that, you know, if you assume, say, an adversarial intelligence service, where English is not the first language, and they are thinking about ways in which they could come up with compelling spear-phishing messages, it is logical to use artificial intelligence of one kind or another to produce a message that could be pretty effective in spear-phishing and, therefore, in taking advantage of vulnerabilities.

And so what we are working on with colleagues across the Intelligence Community are ways of identifying, you know, when that kind of spear-phishing effort is being made using artificial intelligence by a foreign adversary.

Mr. Krishnamoorthi. Thank you.

The Chairman. Mr. Crawford?

Mr. Crawford. Thank you, Mr. Chairman.

Thank you all for being here today.

I have a Wall Street Journal report I want to refer to here. It was published earlier this week, detailing how unprepared, in their view, America is for an era of, quote, "great-power conflict with the likes of China and Russia."

Here is a little bit of their analysis here: Quote, "Decades of ever-bigger military budgets, including a 7-percent boost in spending this year, have improved the lethality of China's air force, missiles, and submarines, and better training has created a more modern force from what was once a military of rural recruits. China is developing weapons and other capabilities to destroy an opponent's satellites, the Pentagon says, and its cyber hacking presents a threat to infrastructure."

Further, a similar report from the Australian Strategic Policy Institute published findings around countries who are leaders in advanced technologies. Forty-four categories measured. Of those 44 categories, the United States led in 7; China led in the balance.

I have that graph. I would ask unanimous consent to enter it into the record.

The Chairman. Without objection.

[The information follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

Mr. Crawford. The study said, quote, "China's research strengths at the intersection of photonic sensors, quantum communications, advanced optical communications, in addition to post-quantum cryptography could mean that intelligence communities, particularly the Five Eyes, could lose important capabilities and suffer from diminished situational awareness. China leads globally in photonic sensors, quantum communications, advanced optical communications, and post-quantum cryptography."

It further states, "Taken together, these observations increase the risk of Chinese communications going dark to the efforts of western intelligence services. This reduces the capacity plan for contingencies in the event of hostilities and tensions," end quote.

Let me ask you, panel: Do you agree or disagree with those statements? And what is your agency -- or agencies, what are you doing to build, catch up, or stay ahead of China, considering those comments?

General Nakasone. Congressman, if I might begin, I would agree that China has shrunk the gap in terms of where they were previously to where they are today.

What is the National Security Agency doing? Several things.

First of all, we play to our competitive advantages. We make code and break code better than anyone in the world.

The second piece is that we look at partnerships. You mentioned the Five Eyes, but it is a broader set of partners that we have to bring in -- academic partners, engage with industry, engage with allies. This is what gives us strength that China will never have.

And the last piece is the close association that we have as a combat support agency with the Department of Defense to identify vulnerabilities, mitigate them, and then ensure that we can advance from them.

General Berrier. Congressman, the Defense Intelligence Agency has recently

reorganized with a China Mission Group that is specifically focused on this threat.

We are continuing to engage our Five Eyes partners and other partners in the region on where we can work together to get after this threat in a collective way. And we will be expanding our footprint into the Indo-Pacific here very, very soon.

Mr. Crawford. Excellent. Thank you.

Any further comments?

Mr. Burns. Sir, just to -- I mean, we have made the same kind of important organizational changes, because I think the two challenges that you just talked about, Congressman, are going to be central to our future as an intelligence service, meaning China in competition with the PRC and then the revolution in technology, which is going to be the main arena for that competition.

So what we have done is stepped up considerably efforts to collect on all the areas that you have described; stepped up our efforts, working with partners in the U.S. Government but also foreign partners as well, to slow down PRC's efforts to try to, you know, gain an advantage in those areas.

And, then, just to underscore what General Nakasone said, what is crucial to all this is working with partners, both in the private sector as well as foreign partners as well.

Mr. Crawford. Excellent.

Let me flag one more issue for your attention. This is also a Wall Street Journal report. "Remote Corner of Taiwan Confronts Wartime Scenario" -- that is the headline -- "Life With No Internet." And the gist of this is, there is an island that had their internet cut off, effectively, and this is typically a precursor for kinetic action.

And the question I have is: With regard to Taiwan, do you think we have adequate redundancies to be able to address that threat, should that situation arise?

Director Haines. I think I will just say generally, this is an issue that we are worrying

about across all of partners, allies, et cetera, is to ensure that we have a way to help them.

And I think we can -- yeah -- further discuss details in closed session.

Mr. Crawford. So that has been the case in Ukraine, where obviously that --

Director Haines. Exactly.

Mr. Crawford. -- diminished their capability for communications and so on, operational control. And that is why I asked the question, because I obviously have some concerns about addressing that. Do we have the adequate resources in place to mitigate that threat?

Thank you, and I yield back.

The Chairman. Mr. Crow?

Mr. Crow. Thank you, Mr. Chairman.

Russia has committed and continues to commit unspeakable war crimes against the Ukrainian people during the conduct of this war.

The United States is not a signatory to the International Criminal Court, but Congress last year passed a law that made it very clear that we should provide intelligence and information related to these crimes to the International Criminal Court.

And I will quote. In the appropriations bill that passed late last year, it allows exceptions allowing for assistance with, quote, "investigations and prosecutions of foreign nationals related to the situation in Ukraine, including to support victims and witnesses," end quote.

And, of course, the discussion around that and the debate around that made it very clear that congressional intent was for the IC to provide that information to the ICC.

It is my understanding that there is debate within the administration -- more specifically, that the Department of Defense is preventing that assistance and that information from being relayed to the ICC, including a principals meeting that occurred on February 3rd,

where there was debate about that.

So, Director Haines, is it your understanding that current law passed by Congress mandates the ICC provide -- or, that the United States -- the IC provide this information to the ICC in furtherance of investigations of Russian war crimes?

Director Haines. Thank you, Congressman.

So we absolutely -- and I don't think there is any debate that we should be providing support to the ICC on Russian war crimes, you know, as a general matter.

What we do is, we provide intelligence that can be provided to the ICC through the arms of the U.S. Government that typically work with the ICC, so the State Department's War Crimes Issues Office. We don't do that directly. And I think, you know, it is really a question for them as to what exactly they are providing and whether or not --

Mr. Crow. So is it your understanding, Director, that there is information that is currently not being provided to the ICC that the Intelligence Community would like or otherwise would provide to the ICC that the Department of Defense and this administration has not allowed to be provided?

Director Haines. No.

Mr. Crow. So there is no dispute about that within the administration?

Director Haines. We provide it to the policy arms. They provide it to the ICC. I don't actually know exactly what they have provided or haven't provided.

Mr. Crow. More specifically, then, is it your understanding that the Department of Defense is holding up the provision of information or intelligence to the ICC?

Director Haines. No.

Mr. Crow. That is not your understanding?

Director Haines. That is not my understanding. I think --

Mr. Crow. Director Burns, do you have an understanding one way or the other on



this?

Mr. Burns. No. Same as Director Haines on that -- on the question you asked, sir.

Mr. Crow. Okay.

The next question is about the assistance generally to Ukraine. There is a lot of debate within Congress right now and with the administration about both the quantity and the quality of the military assistance to Ukraine.

My understanding is that Russia does not have the capability of any major offensives or breakthroughs currently in Ukraine, that they have been degraded sufficiently.

So, Director Burns, is that your understanding, that in 2023 the Russians couldn't conduct major offenses or have major strategic success in Ukraine?

Mr. Burns. Yes, sir. It is our judgment that the Russian military is capable of making incremental tactical gains, and they have made some in the course of the offensive they have launched over the last 4 or 5 weeks in the Donbas in eastern Ukraine. But it is our collective assessment, I think, that, for a whole variety of reasons that Director Haines mentioned -- munitions shortages, morale problems, manpower problems, conflicts within their own military leadership -- that they are unlikely to be able to make significant strategic breakthroughs or sustain them over the course of the rest of this year.

Mr. Crow. And is it your understanding that Vladimir Putin's strategy is to recapitalize the military, to consolidate support, and to rebuild his infrastructure so that he will be capable of making advances or strategic success within 2024 and 2025, that he is taking a longer-term view?

Mr. Burns. Yeah, I think Vladimir Putin is very much taking a longer-term view. I think he is doubling down, in many respects, right now.

I believe he is convinced that he can make time work for him, that he can grind down the Ukrainians through this war of attrition, that he can wear down Western supporters of

Ukraine. And he is convinced also, and has been for some time, that Ukraine matters more to him than to us. Therefore, the challenge, I think, is to puncture that view.

Mr. Crow. So, given that, that decisions have to be made about relative risks and where risks lie, short-term risks versus long-term risks, would it be your best advice that we transition the nature of our support to look more towards hardening Ukraine and military modernization efforts that would look further out in the horizon than the shorter-term efforts?

Mr. Burns. Well, you know, I avoid offering free policy advice in my current role these days. What I would say as a matter of intelligence assessment is that the next several months, the next 4 or 5, 6 months, are going to be crucial on the battlefield in Ukraine. I think any prospect for a serious negotiation, which President Putin I do not believe is ready for today, is going to depend on progress on the battlefield.

Therefore, I think, analytically, what is important is to provide all the support that we possibly can, which is exactly what the President and our Western allies are doing, for the Ukrainians as they prepare for a significant offensive in the spring.

And at the same time -- it is not really an either/or question, just as you said, Congressman -- it is looking at the long-term security needs of Ukraine to help ensure a situation where Vladimir Putin's Russia is not going to try to mount another offensive or another invasion as they did at the beginning of last year.

Mr. Crow. Thank you.

I yield back.

The Chairman. Ms. Stefanik?

Ms. Stefanik. Director Wray, 1 year ago at this very same hearing, I asked you about the deadliest vehicle crash in decades in my district in upstate New York, the 2018 Schoharie limo crash, instantly killing 20 people. Those families have never been the same, and my office has communicated with many of them.

The owner of the illegally retrofitted limo was a longtime FBI informant with a rap sheet a mile long. And it was because of my question to you in this open hearing that the FBI was forced to open an internal review.

Let me be clear: That review was in response to our congressional oversight.

Since then -- that was a year ago -- the FBI has stonewalled and slow-walked our additional requests for updates on that review until, miraculously, just this week, before you knew you were going to appear here today, we received an email informing this committee and myself of the following:

"The internal review is now complete. The FBI will provide a briefing, and, in connection with that briefing, we will make available the internal review with certain redactions. We will coordinate with your staff regarding the in-camera review of the materials. The FBI is providing this briefing and materials with the understanding that the committee will not publicly disclose the nonpublic information contained therein."

My expectation is that briefing will be this month. Do I have your commitment?

Mr. Wray. Yes.

Ms. Stefanik. I want to follow up. Can you commit to providing that briefing to those family members, immediate family members, the parents or spouses of those victims?

Mr. Wray. On that one, let me make sure I talk with our folks and circle back with you about what can be shared, if there are any limitations. Obviously we want to make sure that the victims and their families are appropriately informed, but I don't know yet what constraints there may be. So we will follow back up with you on that one.

Ms. Stefanik. Yeah, they have not been appropriately informed, and it is only because of my work in congressional oversight that they are starting to have sunlight.

I believe you are a parent, Chris Wray?

Mr. Wray. Yes, I am a parent.

Ms. Stefanik. I am a new parent as well. And there is a set of parents that lost three daughters in that crash. So providing sunlight and transparency is important.

I also want to note an important portion of the letter that was included. It says, "The FBI considers the provision of the internal review as fulfillment of the above-referenced fence."

I remind you that this committee, not the FBI, determines the level of transparency equating to full compliance with our constitutionally directed oversight role.

Mr. Chairman, I want to submit this unclassified version of the letter for the record.

The Chairman. So ordered.

[The information follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

Ms. Stefanik. I also want to shift gears here, regarding Judiciary Committee. I serve on the select subcommittee there, and this committee has made 50 different requests for information and documents concerning the operations and the actions of the FBI. And, to date, the FBI has not complied with the Judiciary Committee's long-outstanding request for information and documents.

The FBI is accountable to Congress and, by extension, the American people. Responding to this routine oversight is the bare minimum. And, today, the FBI failed to send a witness to the Judiciary Committee hearing, saying that we had this hearing happening.

Can you commit to sending a witness before the next Judiciary Committee subcommittee hearing on March 28th?

Mr. Wray. We are happy to work with you on making sure we --

Ms. Stefanik. Can you commit to --

Mr. Wray. -- make information available --

Ms. Stefanik. -- provide a witness?

Mr. Wray. We will, of course, make people available to the committee.

Ms. Stefanik. But you didn't make people available today.

Mr. Wray. Well, I --

Ms. Stefanik. This is the base minimum. The agencies need to provide witnesses.

Can I get a commitment, yes, you will provide a witness?

Mr. Wray. We will work with you to make people available.

Ms. Stefanik. That is not a "yes." So, for the American people, you are having the FBI Director refuse to provide a witness? Just say "yes."

Mr. Wray. I am not refusing to provide a witness. I want to be clear on that. I said

we will work with you to make somebody available.

Ms. Stefanik. So, great. So someone will be made available?

Mr. Wray. Yes.

Ms. Stefanik. Yes. Thank you. That is all I wanted, a "yes."

Moving forward, do you believe the Hunter Biden laptop story is disinformation?

Mr. Wray. Well, I want to be careful about -- there is an ongoing investigation that is relevant to that, so I have to be careful about what I can share on that here.

Ms. Stefanik. Do you believe the Hunter Biden laptop story is disinformation?

Mr. Wray. I don't think there is anything I can share on that in open setting.

Ms. Stefanik. Were you aware that the FBI personnel were in contact with Twitter regarding the Hunter Biden laptop story?

Mr. Wray. I don't believe FBI personnel were in contact with Twitter about the Hunter laptop story specifically. I think there were people in contact with Twitter about Russian disinformation efforts.

Ms. Stefanik. Of which the Hunter Biden laptop story was included, according to the FBI.

Mr. Wray. Well, I don't know exactly what you are looking at, but I am happy to talk about what it is the FBI does and does not do with respect to social media companies.

Ms. Stefanik. Were you aware that the FBI had Hunter Biden's laptop since December of 2019?

Mr. Wray. I can't speak to exactly when we had a laptop available. There is a -- as you know, there is an ongoing investigation run by the U.S. attorney out of Delaware from the prior administration that we continue to work very closely with. And our Baltimore --

Ms. Stefanik. And we have an ongoing investigation as well.

Mr. Wray. And our Baltimore Field Office is working very hard with that U.S.

attorney. And I expect them to pursue that case as far as it takes --

Ms. Stefanik. This stonewalling, Director Wray -- the American people deserve answers, and this is unacceptable.

Lastly, did you sign off on the Mar-a-Lago raid?

Mr. Wray. Well, first off, it was not a raid. It was an execution of a search warrant.

Ms. Stefanik. Did you sign --

Mr. Wray. Second --

Ms. Stefanik. -- off on the execution --

Mr. Wray. Second --

Ms. Stefanik. -- of the search warrant?

Mr. Wray. May I finish?

Second, I don't sign off on individual search warrants, in that case or in any other.

Ms. Stefanik. Did Attorney General Merrick Garland sign off, to your awareness?

Mr. Wray. I can't speak to the Attorney General.

Ms. Stefanik. Was there dissent at senior levels of the FBI about the conducting of the search warrant?

Mr. Wray. I can't speak to internal discussions among the FBI or among the FBI and the Department of Justice.

Ms. Stefanik. Even though it has been reported in The Washington Post?

Mr. Wray. There are lots of --

Ms. Stefanik. Multiple --

Mr. Wray. -- things reported in the media --

Ms. Stefanik. I know. Leaked from your agency.

Mr. Wray. [Inaudible.]

Ms. Stefanik. Leaked from your agency --

Mr. Wray. Yeah.

Ms. Stefanik. -- frequently it is reported in The Washington Post.

Mr. Wray. And it may or may not be accurate.

Ms. Stefanik. It may or may not be accurate.

With that, I yield back.

The Chairman. Thank you.

Dr. Bera?

Dr. Bera. Thank you, Mr. Chairman.

You know, in preparation of this briefing, staff gave me a number of questions to ask. And then, lo and behold, yesterday we had a email from the Speaker and Leader Jeffries talking about a data breach at DC Health Link that affects all of us. We all got that.

So let's talk about cybercrime, ransomware, et cetera. I am sure we will get briefed on the data breach in the future, but obviously cybercrime and ransomware is a major issue that we are dealing with and probably becoming much more frequent.

Maybe this is a question for Director Haines or Director Wray.

You know, I was prepared to ask about state actors but also non-state actors. We can harden all of our devices, harden all of our offices, but there are lots of weak links out there.

And, you know, I think, a couple things. How do we work with the private sector to compel them to put in the resources to harden their cyber hygiene?

Number two, how do -- you know, and maybe this is for Director Wray or either one of you: For private-sector companies, small and large ones, how do we compel them to make sure they are working with us, whether it is the IC or, you know, the broader community, to let us know when a ransomware occurs? Because, you know, for us to address this issue, we have to be aware of the issue and we have to, you know, get that information.



So, you know, to whoever is appropriate.

Mr. Wray. So you are exactly right in once sense in particular, that the private sector is the key to all of this. Eighty-five percent of our critical infrastructure is in the hands of the private sector. It is probably a higher percentage of that when you look at our innovation, and an even higher percentage than that when you look at our PII.

As you know, Congress passed, which I think is an important first step, a breach notification bill that will reach critical infrastructure in particular. I think there are things that can be done and should be done to strengthen that to ensure that the information not only is flowing from a broader swath of the private sector but also is flowing more quickly to us so that we can help as quickly as possible.

And then I think, overall, part of it is raising cybersecurity awareness, which is part of what the really active engagement that we are trying to participate in, all of us, with the private sector, is designed to accomplish.

General Nakasone. If I might add, Congressman, it also means being able to leverage what we do as an Intelligence Community, operating outside of the United States, understanding what adversaries are doing, being able to see their tradecraft, being able to share that tradecraft publicly.

This is back to the partnership that is very close between NSA and FBI in terms of, when we see certain things happening there, being able to provide that to the FBI as they talk to U.S. critical infrastructure companies in the United States. And we prioritize that work. That is very, very critical to us.

Dr. Bera. Great. Thank you.

Let me shift directions. A couple weeks ago, I had a chance to go on a bipartisan codel to Japan in my Foreign Affairs capacity. And, clearly, Japan is a geopolitical strategic ally of increasing importance. And, you know, we applaud the Kishida administration for

really stepping up and understanding the new framework.

You know, they brought up in our meetings -- you know, obviously, they are not at Five Eyes, but Five Eyes Plus One, et cetera. But, as we started to talk about their cyber hygiene, you know, the fact that, you know, some of their own laws don't allow them to do security clearances, et cetera -- we want to have this relationship, we want to co-develop products.

What can we do as Congress and then, you know, working with the administration to -- they are very aware of their vulnerabilities on cyber, but it seems like it is moving very slow. And I would be curious.

General Nakasone. So, Congressman, I would welcome to brief you and other members of the committee of what we are doing with Japan and other partners in the Pacific to, as you indicate, raise the bar for cybersecurity.

I think this is instrumental to understanding where we need to go as both the Intelligence Community and select partners. We need to be able to share information with a great assurance that they can protect it. We need to be able to communicate with them with the idea that what we are saying will not be monitored.

These are all things -- and I give the Japanese great credit. Over the past several years, they have done tremendous work. But we do need to focus on this very, very hard going forward.

Dr. Bera. Great.

Director Haines or anyone else?

Director Haines. Yeah, I will just add to what General Nakasone said.

I mean, this is an area of work that we have been engaged with Japan, with the Republic of Korea. We actually have a trilat through which we work together on these kinds of issues.

It is incredibly important, as you say, just to help all of us be better at cybersecurity, but then also to be able to work against, for example, North Korea, others that are engaging in activities that are attacking our systems.

Mr. Burns. And all I would add, Congressman, is that, you know, we share both the admiration for what Prime Minister Kishida and the Japanese leadership is doing now in terms of their national security, which is hugely important to our shared interests.

And I think we also applaud the Japanese leadership for understanding, you know, what we have sometimes learned the hard way in the United States -- it is not as if, you know, we have a monopoly on wisdom on this -- but the importance of improving cybersecurity as well.

And, as an agency, we are working with our partners -- I was last in Tokyo in December, I guess, talking about these issues -- to do as much as we can to be supportive, as the committed allies that we are.

Dr. Bera. Great. Thank you.

And I yield back.

The Chairman. Mr. Kelly?

Mr. Kelly. Thank you, Mr. Chairman.

And thank each of you for being here.

And I want to start off, the men and women who do the work of the IC are amazing men and women, and they protect this Nation on a daily basis. However, I will comment on some of the things that have happened.

There is an erosion of trust in the American public that you are protecting us and protecting all of our constitutional and civil rights that are created through the Constitution, whether that is leaks at high levels to media sources or to put a political viewpoint, which is not necessarily anybody at this table; whether that is resistance to oversight and using, "It is

currently under investigation."

Just understanding, we are not a normal Congressperson. We are selected for this committee. We have had trust emplaced by us by both sides of the aisle to be able to keep and maintain the same secrets that you do.

Whether it is not providing witnesses when we ask for them and saying, "Well, they may not want to be disclosed" -- we have subpoena power. If they don't want to disclose, we can subpoena them.

It is important for us to be able to do our job as partners with you in that oversight. And that is what we want to do, not to throw daggers and rocks at you. But what we want to do is, we are the people who are most charged with selling FISA renewal to the Congress and to the American people, and without proper oversight we can't do that.

As we used to say in the Army, one "oh, crap" does away with 10 years of "attaboys," okay? I mean, we cannot do that. So, when one leak happens, if the public doesn't feel like we are addressing that appropriately, we have to do that.

So I would just ask you, Director Haines: What are we doing for you to help us rebuild the trust in the public that they have lost over years through -- many times it predates you, but it doesn't matter when it happened. We have to turn the perception back, that we trust the FBI, we trust the CIA, we trust the NSA.

Director Haines. Absolutely. Thank you, Congressman.

I think having the trust of the American people with respect to the Intelligence Community is absolutely fundamental, and it is critical to us doing our job, for all of the reasons that you indicated but also so that, when we put out a warning, frankly, that the American people trust it enough to act on it or to be, you know, subject to it.

So what we are doing is, across the board, trying to ensure that we have appropriate oversight over the extraordinary powers that we have.

In the context of 702, I think you have heard a little bit from Director Wray, but, honestly, all of us have a lot to say on this subject.

Really, the investment that we are making in training, in policies and procedures that help to ensure that we are doing things in accordance with the law, that we are looking at designs of technology to ensure that it is actually quite hard to do anything else, we are looking at the oversight process every, you know, 2 months --

Mr. Kelly. Let me -- because I want to get a little more.

Director Haines. Please.

Mr. Kelly. I mean, and I use the raids recently -- and raids, search warrants, whatever -- all the documents, through multiple Presidents and Vice Presidents, that were improperly disclosed. We have to do a better job of not telling the American public all those things, but they have to know, when the SSCI asks for those things and when we ask for those things and you tell us we don't have a need to know or a right to know, I can assure you, that erodes public trust. That does not help.

We are not partisan folks on this committee when we are asking that. We are asking that for oversight. So I would just ask that you comply with those.

And the second thing, I am going to shift a little bit to the Southern Hemisphere, because I know in your Senate hearing you talked quite a lot about the border and those kind of things. We also talked about transnational terrorist organizations and drug cartels and those things.

That is not a kinetic fight, but I would just ask you guys to look at what we as an Intelligence Community and a Title 10 community, what can we do train-and-assist-wise to move to the southern border of Mexico, south -- what can we do to improve our standing in those nations through training and assist or through intelligence provided to them? What can we do to strengthen our relationship so we don't have so much pressure on our border?

Mr. Wray. I will start, and I am sure others will want to weigh in.

I mean, one thing that I would call out -- you rightly said Mexico and then further south. So one of the things that we have been doing that I think we can double-down on -- and we are trying to do that -- is work with the Northern Triangle countries, you know, where you have MS-13, 18th Street Gang, et cetera.

But to illustrate how thorny and complicated this problem is, we have what we call transnational anti-gang task forces in all the three of El Salvador, Honduras, Guatemala. And in El Salvador, recently, for example, working with them, we had a massive MS-13 takedown, which was great. On the one hand, you have got all these people locked up in El Salvador before they got anywhere near the border. The problem is, there is so many of them that the ones that didn't get caught immediately started fleeing, looking for someplace else to go, and guess where they wanted to come? They are heading straight for our border.

So it illustrates why we can't just kind of play whack-a-mole. We have to try to have a comprehensive solution to this problem.

Mr. Kelly. And, Mr. Chairman, I yield back.

The Chairman. Great.

I am going to ask unanimous consent that we go to 4 minutes, not 3 as we would -- but to 4 in order for us to be able to get done to make it to our 1 o'clock.

Ms. Spanberger?

Ms. Spanberger. All right. Thank you so much, Mr. Chairman.

And thank you to everyone who is here.

I proudly serve so many members of the Intelligence Community as their Representative in Congress. And so, on that note, I would like to start with something that has impacted personnel. I would like to begin by --

The Chairman. Could we reset the clock, please?

Ms. Spanberger. -- by saying that I appreciate the outreach that I have received from various agencies knowing of my interest in this.

And the conversation hopefully will continue in closed session, but, in this unclassified document, I would like to just ask for comments on the fact that it literally says what, to me, are somewhat contradictory statements in one paragraph, noting, "It is unlikely that a foreign actor, including Russia, is conducting a sustained worldwide campaign involving hundreds of incidents," related to anomalous health incidents.

Further in the paragraph, it says, "The IC continues to actively investigate the AHI issue, focusing particularly on a subset of priority cases for which it has not ruled out any cause, including the possibility that one or more foreign actors were involved."

There is a lot of consternation among those who have been impacted by AHI. I appreciate the work that you all are doing in making sure people are having their health needs met. But would anyone like to comment on what appears to be, by my reading, somewhat contradictory statements in one small paragraph?

Director Haines. Okay. I will start. No, thank you very much, Congresswoman.

I think there is no question, while, as the analysis that you are looking at indicates, that as a general matter, you know, across the IC, most IC elements now have concluded that it is very unlikely that a foreign adversary is responsible for the reported AHIs. And there are different degrees of confidence associated with that, and then you have some that look at it as unlikely that a foreign adversary, essentially, have done this part.

At the same time -- and this is sort of where, you know, our work continues -- and there is no question that we see this as a continued priority for us -- is that we are going to be and continue to be vigilant about looking for information that undercuts those assumptions, because we recognize there are gaps here.

We are going to continue to focus on trying to understand essentially what it is that we

can do to help the folks that have experienced these very real symptoms and these issues and to figure out what is happening to each of them.

And, as we look at the experts panel that went through a process to look at different mechanisms that might, in fact, be causing different symptoms, issues, and so on, they had recommendations on research and development that would continue to go forward, and that is something that we are also pursuing.

And any remaining questions that we have are things that we are looking to try to ensure that we are focused on, moving forward. And I would just like --

Ms. Spanberger. Well, we are --

Director Haines. Yeah.

Ms. Spanberger. We are currently at a point, is it correct to say, where this is a point-in-time analysis, and the door is very much open and the investigation very much continues, that there could be a reversal, or not, of new information that would cause a new assessment that might differ from what we have seen thus far?

Mr. Burns. Yeah, I guess what I would say, Congresswoman -- first, I have huge respect for your service at the Agency, as well, and to the Intelligence Community. And I would say several things.

Yeah, none of us are pretending that -- I think the thorough and rigorous work that was done, reflected in the Intelligence Community assessment, is -- none of us are pretending that that is absolutely the final word in this.

Ms. Spanberger. Good.

Mr. Burns. We will sustain a dedicated unit of officers at the CIA, working with our partners in the Intelligence Community, not just to be alert to any new leads that could develop but to follow them rigorously.

We will also continue to focus with our partners on research and development efforts



by our adversaries that could focus on directed-energy mechanisms as well.

The only things I would add is, first, from the day I began as Director of CIA more than 2 years ago, I have understood -- I have tried hard to understand the significance of this issue. It is not an abstraction. It is about real people suffering, you know, real health conditions and real pain in the service of their country.

And so we made fundamental improvements in the level and access to care. They will not diminish. We remain committed to, you know, supporting all of our workforce as well, and we will continue to do that.

Ms. Spanberger. Thank you.

If I may pivot quickly -- because I will want to continue the conversation related to this in closed session -- related to fentanyl trafficking, which is impacting communities across the country but certainly within Virginia, can you update the committee on your efforts to combat cartels and the trafficking of fentanyl that we have seen to be so lethal within the United States?

Mr. Burns. I would be glad to start, Congresswoman.

And I will bring this back to the 702 issue too, because it has been a crucial tool in our efforts at CIA to collect foreign intelligence and enable our partners, whether it is in Mexico or our domestic partners in the United States, to take action to help protect Americans against the fentanyl crisis. I will give you a couple of broad examples, anyway.

One is, we have -- first, I should say, we have transformed our approach at the Agency to how we look at this issue, to focus on networks, meaning precursor chemicals, financial flows, you know, the --

Ms. Spanberger. Precursors coming in from China or wherever else --

Mr. Burns. From China and elsewhere. And then also fentanyl, you know, production and processing equipment as well.

702 has been crucial in illuminating that network for us and, therefore, enabling us, for example, just in the last few months, to work with Mexican partners to take some very successful actions against the Sinaloa Cartel, and then also, in another instance, enable us to work with other partners to take significant action against fentanyl production and processing equipment in Mexico and in the United States as well.

Ms. Spanberger. Diverting equipment on those networks?

Mr. Burns. Yes.

Ms. Spanberger. Thank you for that update.

Mr. Chairman, I yield back.

The Chairman. Mr. Fitzpatrick.

Mr. Fitzpatrick. Thank you, Mr. Chairman.

Thank you all for being here and for your service to our Nation.

I just want to ask one question for the panel. It is my personal belief that the biggest challenge facing the Intelligence Community and, therefore, the biggest essential threat facing our Nation is when, unlike 9/11, where we had universal, 100 percent support, we had incredible bipartisanship here in Congress, incredible universal support for the intelligence agencies, when things happen -- and, by the way, in the case of Director Haines, Director Burns, Director Wray, due to the actions of your predecessors, not yourselves; you have been forced to deal with their actions -- when there is a chipping away of that trust, there is -- when we are empaneling juries and conducting jury questioning, there is a way to remove jurors for bias, amongst other things -- the background check system, the polygraphs can screen for drug use, foreign contacts, and the like. But there is really no way that I am aware of -- and I don't know if there is a policy solution -- that we can check for bias.

Because I think the biggest threat to these agencies is when there is a public perception that there is a political bias on the left or the right. It could be both. It used to be

easy to do that when we lived in different times, but our country is very -- you know, hyperpartisanship is at a spike right now. And that invariably bleeds into the hiring process and makes it tough for the agencies to screen for that. So how do you deal with that, right?

I mean, when I was in the Bureau, we rarely, if ever, heard any talk about politics. We really didn't. And I took that as a source of pride for the Bureau. But this was before we have seen the spike in hyperpartisanship.

How do your agencies combat that? Because it really is a risk, because it bleeds into the public not having faith -- in some cases justified, in some cases not -- of the actions of the various agencies.

Mr. Wray. Well, obviously it is a complicated topic. One thing I will point to that we have done -- because I think you are right to focus not just on actual problems, which have occurred, but appearances issues, perceptions. Those things matter. And so one of the things that we did is, I ordered a stand-down to focus on not just objectivity but making sure that we avoided even the appearance of bias.

And so I started in a way that you will, from your past experience, recognize as very unusual at the FBI. Instead of saddling the front lines with some new training requirement because of something somebody else somewhere did, I started at the top.

So I took all 250, or whatever it is, of the SESers, all the way from legat in Australia all the way to California, and made them all come to Quantico for a single day, where the overwhelming message was back to fundamentals, the right thing in the right way, what they heard from judges.

Because a lot of what you are describing about it is sort of trying to adopt more of the kind of mind set that judges have. They may have political backgrounds, but they put those to the side, they check them at the door, when they take on the robe. We need to have that same kind of mentality.

So the point was to start at the top, with everybody at the top of the organization, make them take the medicine first, and then push it out to the workforce. And we did it for the entire workforce.

Director Haines. Can I just add to that? Just to say that I think this is a critical issue. And I think, Congressman, you know, as you think about this, if you have ideas for us, please let us know.

I see this as, first of all, from a leadership perspective, setting the tone for a culture that makes clear that, just as you described your prior experience in government, that politics have no place in the workspace and in national security, that this is something that -- you know, I also grew up as a civil servant in the government, and nobody asked me what party I belonged to. That was never an issue. And that is something that just has no place in our work.

And I think we are looking -- you know, as Director Wray's comments made clear, like, across the Intelligence Community, all of us, I think, feel very strongly about setting that tone for culture and making sure that that is not an issue.

I think the second piece for the IC more generally is, in fact, engaging in greater transparency where we can. And I think exposing our assessments, doing an Annual Threat Assessment world hearing in an open forum, as you have asked us to come back and do, trying to put out more of our products, trying to give an opportunity for the American people to see the work that we do, sort of, you know, to give a little bit more insight into how it is that we do things, can help.

And then, finally, in the context of transparency, giving more of a sense of the rules within which we operate and do not. And that is something that we are continuing to try to push out, frameworks and ways of working and compliance things, to expose when we make mistakes and when we don't and what we are doing about it.

The Chairman. Director, we are going to have to move on, if you don't mind holding your comments. Great.

Mr. Crenshaw?

Mr. Crenshaw. Thank you, Chairman.

And thank you all for being here.

And, look, I think you are all very serious security professionals, intelligence professionals, and I think that most of this report certainly reflects that.

But there is a glaring exception to that, and specifically in the section on climate change and environmental degradation. Now, don't get me wrong; I think this is indeed an issue. But I address this issue on a very different committee, not here, and for very good reason.

So I have a simple question: What creates greater geopolitical instability? Is it the occasional severe weather event, or is it energy insecurity -- in other words, the inability of nations to secure reliable and affordable sources of energy? Which one creates more global chaos and, therefore, represents a national security threat to the United States? Is it one or the other or both?

I suppose I will direct that question -- I am sorry, but to you, Director Haines, because you mentioned it earlier.

Director Haines. No. Thank you, sir.

So --

Mr. Crenshaw. One or the other or both? Because I have a lot to say on this.

Director Haines. I don't have a way of quantifying it for you. So I am happy to try to take that for the record, if that is useful.

Mr. Crenshaw. Okay.

[The information follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

Mr. Crenshaw. Let's assume that, you know, you try to say both or one or the other, but the report only says one. The report only says one. But if it was both, then why wouldn't energy scarcity be mentioned as a global threat? Why isn't radical environmentalism mentioned as a global threat?

The last few years have some pretty glaring examples, and I am going to point them out in my limited time here.

In Sri Lanka, radical environmentalist policies led to the collapse of farming outputs and the collapse of a government. The same thing is currently happening in the Netherlands, where their entire farming industry is under threat.

In Pakistan, your report mentions some flooding but says nothing of the hundreds of millions of people without power because of energy scarcity due to foolish green-energy policies by the Europeans that have made natural gas so unaffordable in countries like Pakistan.

European energy prices have gone through the roof, and they now desperately import coal and wood to burn because they engaged in misguided green-energy policies for years.

The WHO estimates that 3 million deaths result per year from lack of clean cooking fuels, meaning they are burning wood or dung instead of fossil fuels like propane and natural gas.

These things are truly destabilizing the global security, but there isn't a section in this report about it.

The report does say that it is weather events that are a national security threat and that tensions will rise as developing nations request reparations from developed nations.

Of course, the assumption is that all weather events are due to climate change. That is not science, by the way. It is an assumption. And I wouldn't expect assumptions from

senior intelligence professionals.

It is worth examining the actual science. Has anybody read the U.N. Intergovernmental Panel on Climate Change Report, all 4,000 pages?

Ah, really? Okay. But let's assume you have. It has some good data in it, actually. I like that report. And it would help this report be more objective.

For instance, it actually makes science-based predictions about what the true economic cost of climate change will be over the next hundred years. It says, "The cost of climate change by the year 2100 will be a 4.5-percent reduction in global GDP from what it otherwise would be" -- not from what it is now -- "from what it otherwise would be."

So, if we go on our trend of growth, we would grow global GDP by 450 percent. With the cost of climate change, make that maybe 434 percent. That is not a national security threat, and I am sure you all agree with that.

The report also states that "insured losses due to catastrophes from climate change have increased 250 percent in the past 30 years."

That is a fact taken way out of context. It is misleading. And, again, I wouldn't expect it from intelligence professionals. Because the obvious explanation is that there are more homes and more infrastructure built on coastal areas.

The truth is, the facts are, that the deaths from natural disasters have decreased 90 percent over the last hundred years.

The truth is that the trend in accumulated cyclonic energy, a metric that captures frequency, duration, intensity of global hurricane activity, shows no increasing in trends. In 2021, we had the fewest hurricanes since satellite tracking began 40 years ago. NOAA modeling shows that hurricanes making landfall will decrease 25 percent as the climate changes.

The U.N. report, the science, never says "red alert," never says "crisis," never says any



of this stuff commonly used by climate alarmists.

I am running out of time, so I just want to summarize, if the chairman will let me.

When we say this kind of stuff, we detract from the very important topics that you all have been talking about this entire time. We detract from that. And it is even worse when we don't at least balance it with the more obvious threat of energy insecurity globally and the destabilizing effects that that creates.

That is my problem with this report, and I hope we fix it next time.

And I yield back. Thank you.

The Chairman. Mr. Hill?

Mr. Hill. Thank you, Mr. Chairman.

And thank the panel so much for being here in this important open testimony for the American people to hear directly from you.

Appreciate, Mr. Wray, your candid responses to the questions.

Director Haines, you started out in your statement, and you were talking about the slowing in Chinese economic growth, and you stated that China now faced some domestic economic challenges.

So I would like -- what is your assessment of what those primary domestic economic challenges for the PRC are? How do you assess that slowing, that economic vulnerability in China?

Director Haines. Thank you, Congressman.

I would just -- I would point to a few here. So one is -- these are sort of structural issues that I think are going to be a challenge for China moving forward.

One is, their population, basically, their aging population. So they peaked in 2021, and last year they declined by 850,000 people. It is the largest decline in over 60 years. And with a relatively low fertility rate, China's population will continue to shrink even as it

ages. And this is going to reduce China's labor force and likely increase expenditures on age-related health issues as they are going forward.

I think a second piece of this is sort of looking at -- the domestic migrant workers' wages in China in low-skilled industries have more than doubled, on average, as the quantity of migrant labor from rural areas has actually declined. And this has contributed to several major domestic and foreign firms' decisions actually to relocate their firms from China to lower-wage countries, such as Vietnam, or to, you know, eschew expansion plans in China, leaving large numbers of China's low-skilled workers unemployed.

And then, furthermore, China is going to need to improve education and training, really, to better prepare its workforce. And at least 100 million low-skilled workers risk losing their jobs as a result of automation that they are pursuing. And vocational education to sort of upskill the untrained rural labor faces really entrenched obstacles within China.

So these are some of the issues that we are looking at that sort of make it a particularly challenging environment. And we think they are going to continue to sort of pursue their, you know, statist economic policies so that state direction is a part of it, which will not be as efficient, essentially, in their moving forward.

Mr. Hill. Well, and a followup to that: Do you assess that in their last 15 years of extraordinary space and defense technology buildup that that workforce is aging? In other words, it has a median age higher than, you know, our baby boom generation. Therefore, they even have vulnerability in their defense/space technological base, because they have an aging workforce there? Or is that a younger-than-average workforce? What is your assessment there?

Director Haines. I don't know the answer to that. I will find out.

Mr. Hill. Thank you.

Director Burns, you know, in open-source information, there is a lot of conversation

about how effective the crypto criminals in DPRK, in North Korea, are about stealing cryptocurrency from wallets around the world. And that is, in turn, many times their export earnings, or what we know to be their export earnings. I think most of their earnings are stolen, so it is kind of hard to gauge what those might be.

What is the United States doing to interdict and block and stop the illicit flows to North Korea through that mechanism?

Mr. Burns. Well, I appreciate very much the question, and maybe we can go into this in a little more detail in the closed session.

But, as we discussed when you came out to headquarters, this is a significant priority for us right now, and I know it is shared across the Intelligence Community, because the North Korean regime does look at just what you described as a way of sustaining itself, of, you know, acquiring revenue as well.

So there are a number of things that we can do, working with some of our allies, to counter that, but I --

Mr. Hill. Good.

Mr. Burns. -- would prefer to talk about that --

Mr. Hill. Thank you.

I yield back, Mr. Chairman.

The Chairman. The list is currently Garcia, Waltz, Scott.

Mr. Garcia?

Mr. Garcia. Thank you, Mr. Chairman.

I want to thank the witnesses. This has actually been a very enlightening and, frankly, clarifying couple of hours for me but, I think, in a most disappointing way.

I have been personally baffled over the last 2 years about our southern border policies coming out of this administration, where in the last year we had 30 times the number of

people die as a result of fentanyl poisonings than folks died during the 9/11 event. Today, more people in our country will die of fentanyl poisoning than Americans died overseas in 1 day of World War II operations.

And what is enlightening to me is that we didn't spend almost any time on this topic today, except for the questions that have been posed to you. I read the 39 pages of the ATA, the 15 minutes of your testimony, Director Haines, and really no mention of these things. You talk about misperceptions of U.S. policies, when we are actually being actively invaded on our southern border right now as a result of this administration's policies.

So what is clarifying to me is the fact that we are sitting here with five people with billets such as Director of National Intelligence, Director of Central Intelligence, Director of National Security Agency, Director of Defense Intelligence Agency, and the FBI, and you guys aren't messaging this as the number-one threat.

I look at your table of contents within the Annual Threat Assessment. You have got China, Russia, Iran, North Korea, climate change, health security, developments in technology, transnational organizations, global terrorism, and the like. And I agree with these topics, and I want to put a boot on the throat of Russia, China, North Korea, and Iran just as much as anyone else. But this is -- it is a shame that the fact that these poisonings right now that you characterize as overdoses and the migration challenges, as you say, Director Haines -- which are not migration challenges; this is an active invasion of our southern border -- are being characterized by this body.

It is indicative to me that you are not briefing the President of the United States on these issues correctly and that you are not putting the proper emphasis on the fact that we are being invaded and Americans are dying at a higher rate than Americans died in World War II on a daily basis as a result of these policies. That is why these policies haven't changed. Very clarifying to me today, based on your testimony as well as the ATA.

On a separate subject, Director Haines, I want to ask you -- well, first of all, I want to ask you what you mean by "misperception of U.S. policies" when it comes to our southern border. And I will let you address that, as quickly as you can, please.

Director Haines. Thank you, Congressman.

I apologize if I gave you a misimpression that we do not believe that counternarcotics is a critical aspect of our work and that it is a priority for the Intelligence Community.

Mr. Garcia. Not counternar- -- not to interrupt, it is not counternarcotics. It is security of our homeland, defense of our southern border that is not the priority, you didn't give me the perception. You have given the American people that perception, and your Annual Threat Assessment reflects that. And, frankly, we will look at your budgets. I am an appropriator for the Justice Department. I will look at your budgets to see if it reflects that priority here shortly.

But, sorry, go ahead and continue.

Director Haines. No. I just want you to know that that is a priority from our perspective.

I think, on the border, we actually, you know, obviously, support and facilitate the United States Government Terrorism Watchlisting process. We have parts of our -- even in ODNI, NCTC, the National Counterterrorism Center, serves as the USG's central and shared knowledge, basically, on known and suspected terrorists. And we maintain TIDE.

And we do a lot of work to try to ensure that all of the intelligence we have is provided to our border agents and to the Department of Homeland Security for the work that they do.

Mr. Garcia. Reclaiming the last 10 seconds, it is a priority. I would submit that it needs to be your number-one priority. And as a mission right now, we are failing. This is a war that we are currently losing and at the rate of 100,000 American lives every year.

So I will defer my technical questions for the classified setting, but thank you guys.

The Chairman. Mr. Waltz?

Mr. Waltz. Thank you, Mr. Chairman.

Just to build on Mr. Garcia's questions, Director Wray, if ISIS or al-Qa'ida poisoned through chemical warfare 70,000 to 80,000 Americans, would we approach that as a law enforcement problem or a military/national security problem?

Mr. Wray. I think we would approach it as all of the above.

Mr. Waltz. So you would use -- certainly we would use military assets, whether it is cyber, space, what have you? You have the authorization, through the authorization of use of military force, to do so, correct?

Mr. Wray. That is my understanding.

Mr. Waltz. You would also have the authorization to use military resources against the Sinaloa and Jalisco Cartels if you had that authorization, use of military force, correct?

Mr. Wray. I believe so, although now you are getting a little bit out of my area of expertise, but --

Mr. Waltz. Would you welcome additional -- for example, offensive cyber from CYBERCOM, would you welcome those additional resources?

We know how to deconstruct cartels, terrorist organizations. We did it in the 1990s in Colombia without a single American combat troop on the ground, and we can do it again now. Would you welcome those additional resources?

Mr. Wray. Well, you will never find an FBI Director that won't welcome more --

Mr. Waltz. I know.

Mr. Wray. -- tools in the fight.

Mr. Waltz. All right. That is good to hear.

Just switching tacks, Director Haines, is ISIS and al-Qa'ida's capability increasing in

Afghanistan right now in terms of their capability to attack the West, attack U.S. interests overseas, influence attacks in the United States, or even potentially attack the homeland? Are they increasing?

Director Haines. So I wouldn't characterize them as increasing, although I would say certainly --

Mr. Waltz. They still have the intent.

Director Haines. -- we have al-Qa'ida and -- yes. For ISIS-K in particular in Afghanistan, they still have the intent. But we can obviously go further, you know, in closed session on details.

Mr. Waltz. Have our collection capabilities since the summer of 2021 decreased in Afghanistan and in the surrounding region?

Director Haines. Certainly with the removal of the U.S. troops and presence in Afghanistan, absolutely, our, you know, collection, day to day, has decreased, although I think, again, we can talk about --

Mr. Waltz. You still have the groups that had the intent to attack us. I am hearing --

Director Haines. But I think we can talk about what our collection posture is vis-à-vis those groups in Afghanistan in closed session and, I think, can give you some comfort on that issue.

Mr. Burns. And -- I am sorry, Congressman. All I would add is, you know, of course it is true, you are right, our capabilities are not the same as when we had, you know, a lot of presence on the ground. However, you know, as we have all promised you over the last couple years, we work incredibly hard to try to ensure that we can still take action, as the U.S. Government did against Ayman al-Zawahiri --

Mr. Waltz. I will look forward to the closed session. However, you are going to have a hard time convincing me that managing sources by Zoom or remotely without being

on the ground is anywhere near as effective.

General Berrier, would the Chinese Communist Party, would Beijing take note if we had an air base a couple hundred miles from their western border?

General Berrier. Yes, I believe they would.

Mr. Waltz. A 12,000-foot runway that we could potentially stage strategic assets a few hundred miles from their massive nuclear buildup?

General Berrier. Yes, I believe they would.

Mr. Waltz. Do you think -- I know this is a bit speculative. Do you think, if the Chinese had a 12,000-foot runway a few hundred miles from the U.S. border, they would give it up for free?

General Berrier. No.

Mr. Waltz. They would protect that asset, right? But we gave up Bagram Air Base. We no longer have access to that air base. Is that correct?

General Berrier. That is correct.

Mr. Waltz. And the British Government is now in negotiations to potentially -- we could potentially lose access to Diego Garcia. Would that be significant?

General Berrier. That would be significant.

Mr. Waltz. Finally, Director Wray, you rightly sounded the alarm bell of opening a counterintelligence investigation every 12 hours with the Director of MI-5.

The National Science Foundation has had a 1,000-percent increase in referrals for grant theft, fraud theft, research theft, yet -- can you just answer me -- I am out of time -- for the record on shutting down the China initiative, or rebranding it, renaming it, and, at least from many people's perspective, diminishing it in priority? Just get that for the record.

Mr. Wray. Well, I can't speak to the Justice Department's initiative itself. All I can tell you is that, at the FBI, we are not taking our foot off the gas one iota on the threat posed



by the Chinese Communist Party, including in the IP sector.

Mr. Waltz. If we are not prosecuting with the same fervor, then that is an issue.

Mr. Wray. Well, I think we are going to try to use every tool in the toolbox that we have. That will include criminal prosecutions when we can do that. That will include other things when we wouldn't do that.

Mr. Waltz. Thank you, Mr. Chairman.

The Chairman. Mr. Scott?

Mr. Scott. Thank you, Mr. Chairman.

Director Wray, I am from Georgia. You have been there the last several years.

Twenty years ago, if you looked at the list of groups the SPLC would have said were hate groups, those groups would have been proud to have been named by them, and I think most Americans would have agreed with the list that they put out.

Today, they put out lists with names like the American Family Association, the Alliance Defending Freedom. And yet one of their attorneys was just recently charged in Atlanta with domestic terrorism. It bothers me to see them cited as a source from your agency on who is and is not considered a domestic terrorist.

Can you speak to the relationship between the FBI and the influence that the SPLC has? Is it just a list that you look at from time to time, or is there coordination?

Mr. Wray. Well, first off, just to be clear, I have considered Georgia my home since --

Mr. Scott. Okay.

Mr. Wray. -- since I first got married, you know, back in 1989. So we have that in common.

Second, as to the product that you are referring to, the intelligence product, when I first saw it -- and I said this yesterday -- I was aghast. It was a single --

Mr. Scott. Okay.

Mr. Wray. -- piece of an intelligence product by one field office. It did not meet our standards, and I --

Mr. Scott. Okay.

Mr. Wray. -- had it immediately removed and withdrawn. And we have taken --

Mr. Scott. Okay.

Mr. Wray. -- steps to make sure it doesn't happen again. And --

Mr. Scott. Thank you.

Mr. Wray. -- one of the reasons I say that --

Mr. Scott. Okay.

Mr. Wray. -- one of the ways in which I say that is the sourcing --

Mr. Scott. Thank you.

Mr. Wray. -- to your question, the sourcing didn't meet our standards.

Mr. Scott. Thank you.

You represent an agency that for years I held in the highest regard. I will tell you, I lost a lot of respect for the Justice Department and the FBI with what happened in a certain case in Valdosta, where there was absolute evidence that a man and two kids had absolutely nothing to do with the death of another individual. That man happened to be an FBI agent. And while he and his family were all cleared by State, local, and the FBI said, "Nothing happened here," there was indisputable evidence.

The U.S. Attorney's Office in Washington, D.C., carried out a civil rights investigation for over 2-1/2 years. And while that family was getting death threats repeatedly because of that investigation continuing to stay open, the U.S. Attorney's Office refused to release the absolute evidence of where all three individuals were.

What can be done to ensure that the U.S. Attorney's Office is held accountable when

they take actions like that that put Americans at risk, especially in this case? It was an FBI agent and his family.

Mr. Wray. Well, I confess I am not familiar with the specific case. In general, speaking just in general, when there are disciplinary violations by prosecutors, there is something called OPR, the --

Mr. Scott. Okay.

Mr. Wray. -- Office of Professional Responsibility --

Mr. Scott. I am going to move on, then. I am going to speak with you. We are going to get familiar with that case. Because I think -- I think that the agents would like for you to probably be familiar with that case.

China flew its spy balloon across the United States, and less than 15 days later, Ford Motor Company, one of America's most iconic brands, said they were going to team with CATL technology to develop a multibillion-dollar battery plant.

Director Haines, is it time for us to declassify a lot of the information that we have on China, their espionage, and what they are doing to Americans and our industry so that we can explain to corporate America that you have to break your ties with Communist China?

Director Haines. Thank you, sir.

We do actually and have been continuing to try to declassify as much information as we can on these issues so as to ensure that corporate America has everything that they need to protect themselves.

Mr. Scott. The key to not going to war with China is for corporate America to understand they have to dual-source or multisource and get out of there.

With that, I yield the 2 seconds.

And, Director Wray, sir, I hate to cut you off, but I am on that clock.

The Chairman. Mr. Gallagher?

Mr. Gallagher. Thank you. I apologize for being late.

Director Wray, yesterday, you expressed certain about the CCP's ability through its ownership of ByteDance to control narratives, software, data on TikTok.

So long as ByteDance or another Chinese entity owns or maintains control of TikTok or its algorithm, would you maintain those concerns?

Mr. Wray. Yes. It is the ownership of the CCP that fundamentally cuts across all those concerns.

Mr. Gallagher. And specifically ownership of the algorithm and control of the algorithm?

Mr. Wray. Well, it is control of the algorithm, it is access to the data, and it is control of the software which allows access to the devices.

So you have a data collection issue, which could be used to conduct all kinds of data operations and traditional espionage.

It is the algorithm, as you have rightly pointed out, that enables them to conduct influence operations. And as I said in response to an earlier question, that is particularly concerning because it is not at all clear we would be able to detect that.

And then, third and finally, it is the control of the software, which gives them access to millions of devices. And all you have to do is look at the fact that the Chinese Government has the biggest hacking program in the world, bigger than that of every other major nation combined. Put that together with the fact that they have stolen more of Americans' personal and corporate data than every nation, big or small, combined. And you put that together with the risks that you and I are talking about, and, to me, it highlights what a big concern this is.

Mr. Gallagher. So I guess the question is, for all of you -- I am just going to go down the line -- simply, should we ban TikTok or force the sale of them to an American

company?

Mr. Wray. Well, I have expressed my concerns. I am not sure how else the problem could be solved, but I have expressed my concerns, which are the ownership of the CCP.

Mr. Gallagher. Is that a "yes"?

Mr. Wray. Again, I don't speak to bans. That is not ultimately my -- that is a policy decision. That is kind of beyond my --

Mr. Gallagher. You all have a voice in the CFIUS process, correct?

Mr. Wray. And we are absolutely -- I know that we are -- I think we all are expressing our assessments of the intelligence, the risk of threats in the CFIUS process. But the ultimate decision about that is, you know, beyond the scope of --

Mr. Gallagher. So, in that process, you haven't been asked "yes or no" yet to --

Mr. Wray. Well, again, we submit our intelligence to the other participants, and then there is a committee that does its work.

Mr. Gallagher. Director Burns, sorry to be obtuse. Should we ban or force the sale of TikTok to an American company?

Mr. Burns. All I would say, Congressman, is I absolutely share the concerns that Director Wray has mentioned, but, you know, we are not in the business of, you know, making policy calls on bans or no bans. But I absolutely share the concerns, and we are not shy about expressing those concerns.

Mr. Gallagher. So, in the CFIUS process, you don't get asked for a recommendation one way or the other?

Mr. Wray. Well, speaking for the FBI, we are asked to submit our intelligence assessment, but we are not asked for -- at least it has been my experience that we are not asked for, like, a recommendation about what the ultimate decision should be.

Mr. Gallagher. Director Haines? Same question.

Director Haines. Yeah. We do not provide a recommendation. Essentially, as Director Wray is indicating, what happens is, our office pulls together the intelligence from the Intelligence Community that is relevant to any particular CFIUS transaction, and we provide that into the process essentially as, you know, grounds for policy discussion.

Mr. Gallagher. Do you share Director Wray's concerns?

Director Haines. I do share the concerns. I share the concerns of foreign-entity-owned social media platforms, other things, that can, you know, be misused, effectively.

And we have a National OPSEC Program, is what we call it. The National Counterintelligence and Security Center runs this. And they have issued guidance, essentially, on the use of these kinds of, you know, applications and platforms.

Mr. Gallagher. General Nakasone, do you share Director Wray's concerns? Are you --

General Nakasone. Certainly.

Mr. Gallagher. -- willing to answer the question of whether we have --

General Nakasone. Certainly. One-third of Americans get their news from TikTok every single day. One-sixth of American youth say they are constantly on TikTok. That is a loaded gun, Congressman.

And, as you know, we are executing, for us, the work to ensure that TikTok is not on government applications and IT.

Mr. Gallagher. I am presently out of time, but go for it, General Berrier.

General Berrier. I would just say we support the CFIUS process. And as we brief decisionmakers and policymakers with the intelligence we have, our analysts are in active and open dialogue. If their opinions are asked, they will give those opinions.

I agree with everything that has been said here. And I have a deputy director who

has three teenagers. If TikTok goes, she may not be able to go home.

Mr. Gallagher. Thank you.

The Chairman. In closing, pursuant to 707, Foreign Intelligence Surveillance Act, 50 U.S.C. 1881a and f(A)(b)(1), you all provide to us annually a list of the -- the characterization of potential abuses of FISA.

Director Wray, your answer to Congressman LaHood was that you have undertaken reforms internally and that you believe it would significantly reduce the overall abuses that we are all concerned about in the FBI.

Anticipating that that might be your answer, we have a letter for you that we will be presenting at the end of the hearing requesting that you go back and look at all of the reports that we have received that indicate those abuses and provide us -- because it is going to be important to our working group -- how those abuses that are identified would have been addressed under your new reforms so that we can find out what is remaining.

And, if there is no objection, I ask that this letter be entered into the record.

No objection.

[The information follows:]

\*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

The Chairman. Thank you all. You continue to show your professionalism and expertise in your answers, and we look forward to continuing to working with you.

We will be adjourned.

[Whereupon, at 12:28 p.m., the committee was adjourned.]



~~TOP SECRET//SI//ORCON//NOFORN~~



**(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE**

**(U) Reporting Period: 01 December 2019 – 31 May 2020**

December 2021

Classified By: [REDACTED]  
Derived From: [REDACTED]  
Declassify On: [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

**(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND  
GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN  
INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL  
AND THE DIRECTOR OF NATIONAL INTELLIGENCE**

**December 2021**

**(U) TABLE OF CONTENTS**

<b>(U) Executive Summary</b>	1
<b>(U) Section 1: Introduction</b>	4
<b>(U) Section 2: Oversight of the Implementation of Section 702</b>	7
(U) I. Joint Oversight of NSA	7
(U) II. Joint Oversight of FBI	10
(U) III. Joint Oversight of CIA	13
(U) IV. Joint Oversight of NCTC	15
(U) V. Interagency/Programmatic Oversight	16
(U) VI. Training	17
<b>(U) Section 3: Trends in Section 702 Targeting and Minimization</b>	19
(U) I. Trends in NSA Targeting and Minimization	19
(U) II. Trends in FBI Targeting	24
(U) III. Trends in CIA Minimization	26
(U) IV. Trends in NCTC Minimization	28
<b>(U) Section 4: Compliance Assessment – Findings</b>	30
(U) I. Compliance Incidents – General	31
(U) II. Review of Compliance Incidents – NSA Targeting, Minimization, and Querying Procedures	46
(U) III. Review of Compliance Incidents – FBI Targeting, Minimization, and Querying Procedures	55
(U) IV. Review of Compliance Incidents – CIA Minimization and Querying Procedures	64
(U) V. Review of Compliance Incidents – NCTC Minimization and Querying Procedures	65
(U) VI. Review of Compliance Incidents – Provider Errors	65
<b>(U) Section 5: Conclusion</b>	66
<b>(U) Appendix</b>	A-1

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(This 2-Page Fact Sheet is Unclassified When Separated from this Assessment.)

(U) **FACT SHEET**

(U) **Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA) Joint Assessments**

(U) This Fact Sheet provides an overview of the *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. These assessments are commonly referred to as “joint assessments,” and are submitted by the Attorney General and the Director of National Intelligence (DNI). As of December 2021, twenty-four joint assessments have been submitted.

(U) **Joint Assessment Basics:**

- (U) *Why is the joint assessment required?* The FISA Amendments Act of 2008 (50 U.S.C. § 1881a(m)(1)) requires the Attorney General and the DNI to assess compliance with certain procedures and guidelines issued pursuant to FISA Section 702.
- (U) *What period is covered by a joint assessment?* Each joint assessment covers a six-month period: 01 December through 31 May or 01 June through 30 November. This joint assessment covers the period from 01 December 2019 through 31 May 2020.
- (U) *Who receives it?* Each joint assessment is submitted to the following oversight entities: the Foreign Intelligence Surveillance Court (FISC), relevant congressional committees, and the Privacy and Civil Liberties Oversight Board (PCLOB).
- (U) *What is being assessed?* The Attorney General and the DNI jointly assess the Government’s compliance with Attorney General Guidelines and with FISC-approved “targeting,” “minimization,” and “querying” procedures.
- (U) *What are targeting, minimization, and querying procedures?* Section 702 allows for the targeting of (i) non-United States persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. To ensure that all three requirements are appropriately met, Section 702 requires targeting procedures. Targeting is effectuated by tasking communications facilities (such as telephone numbers and electronic communications accounts) to U.S. electronic communications service providers. Section 702 also requires minimization procedures to minimize and protect any non-public information of United States persons that may be incidentally collected when appropriately targeting non-United States persons abroad for foreign intelligence information. Querying procedures set rules for using United States person and non-United States person identifiers to query Section 702-acquired information.
- (U) *What compliance and oversight efforts underlie the joint assessment?* Agencies employ extensive compliance measures to implement Section 702 in accordance with procedural, statutory, judicial, and constitutional requirements. A joint oversight team consisting of experts from the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) oversees these measures. Each incident of non-compliance (*i.e.*, compliance incident) is documented, reviewed by the joint oversight team, remediated, and

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

reported to the FISC and relevant congressional committees. The joint assessment summarizes trends and assesses compliance (including calculating the compliance incident rate for the relevant reporting period) and may include recommendations to help prevent compliance incidents or increase transparency.

- *(U) What government agencies are involved with implementing Section 702?* The National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Counterterrorism Center (NCTC). Each joint assessment discusses how these agencies implement the authority.
- *(U) Why is the joint assessment classified?* The joint assessment is classified to allow the Government to provide the FISC, the congressional oversight committees, and the PCLOB a complete assessment of the Section 702 program, while at the same time protecting sources and methods. They are carefully redacted for public release in the interest of transparency.
- *(U) What is the format of the joint assessment?* The joint assessment generally contains an Executive Summary, five sections, and an Appendix. Sections 1 and 5 provide an introduction and conclusion. Section 2 details internal compliance efforts by the agencies that implement Section 702, interagency oversight, training efforts, and efforts to improve the implementation of Section 702. Section 3 compiles and presents data acquired from compliance reviews of the targeting and minimization procedures. Section 4 describes compliance trends. The joint assessment describes the extensive measures undertaken by the Government to ensure compliance with court-approved targeting, minimization, and querying procedures; to accurately identify, record, and correct errors; to take responsive actions to remove any erroneously obtained data; and to minimize the chances that mistakes will re-occur.
- *(U) What are the types of compliance incidents discussed?* Generally, the joint assessment groups incidents into six or seven categories. Categories 1-4 (tasking incidents, detasking incidents, notification delays, and documentation errors) discuss non-compliance with targeting procedures. Category 5 discusses incidents of non-compliance with minimization procedures, such as improper dissemination of information acquired pursuant to Section 702, and querying procedures, such as non-compliant queries of Section 702-acquired information using United States person identifiers. When appropriate, a category discussing incidents of overcollection is included. Additionally, the last category is a catch-all category for incidents that do not fall into one of the other categories. The actual number of the compliance incidents is classified; the percentage breakdown of those incidents is unclassified and reported in the joint assessment. Additionally, because Section 702 collection occurs with the assistance of U.S. electronic communications service providers who receive a Section 702(i) directive, the joint assessment includes a review of any compliance incidents by such service providers.

*(This 2-Page Fact Sheet is Unclassified When Separated from this Assessment.)*

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

**(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence**

**December 2021**

**(U) Reporting Period: 01 December 2019 – 31 May 2020**

**(U) EXECUTIVE SUMMARY**

(U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 *et seq.*, as amended, requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to FISA Section 702 (hereinafter, “Section 702”), and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. Section 702 authorizes, subject to restrictions imposed by the statute and required targeting, minimization, and querying procedures, the targeting of non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. The present assessment sets forth the twenty-fourth joint compliance assessment of the Section 702 program. This assessment covers the period from 01 December 2019 through 31 May 2020 (hereinafter, the “reporting period”) and accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act as required by Section 707(b)(1) of FISA (hereinafter, the “Section 707 Report”). The Department of Justice (DOJ) submitted the Section 707 Report on 04 September 2020; it covers the same reporting period as the joint assessment.

(U) This joint assessment is based upon the compliance assessment activities that have been conducted by a joint oversight team consisting of experts from DOJ’s National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) (hereinafter, the “joint oversight team”).

(U) This joint assessment finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes are in place to implement these authorities and to impose internal controls for compliance and verification purposes.

(U) However, notwithstanding a focused and concerted effort by Federal Bureau of Investigation (FBI) personnel to comply with the requirements of Section 702, misunderstandings regarding FBI’s systems and FBI’s querying procedures caused a large number of query errors. In particular, a single multifactor query at one field office accounted for a significant number of compliance incidents during this reporting period. Even so, the numbers of FBI query errors, and FBI compliance incidents overall, reported during this reporting period were significantly lower than they have been in the past few reporting periods.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

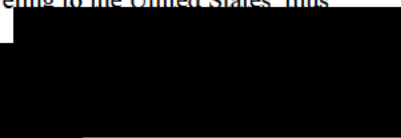
(U) As the below metrics illustrate, this reporting period, almost half of which occurred during the coronavirus pandemic, saw a significant decrease in the total number of identified compliance incidents. At the time of writing this joint assessment, the joint oversight team is not able to determine to what extent these compliance trends reflect a decrease in the number of compliance incidents that occurred<sup>1</sup> – whether as a result of the coronavirus pandemic or other factors – as opposed to difficulties in discovering and reporting compliance incidents as a result of the pandemic. As it pertains to the latter, NSD and ODNI's onsite reviews were affected by the pandemic during the latter part of this reporting period. Specifically, during the latter part of the reporting period, NSD and ODNI postponed some of their onsite reviews at the National Security Agency (NSA); temporarily suspended their onsite reviews at the Central Intelligence Agency (CIA), FBI, and the National Counterterrorism Center (NCTC) (such reviews were ultimately conducted remotely instead); and suspended reviews at FBI field offices.

(U) During this reporting period, the overall compliance incident rate – calculated as the total number of compliance incidents reported during the relevant reporting period, expressed as a percentage of the average number of facilities tasked for acquisition on any given day during the reporting period – was 0.46 percent, which represents a significant decrease from the prior period (20.28 percent).<sup>2</sup>

(U) This assessment also includes the targeting compliance incident rate for NSA (see Figure 14, pg. 38), which represents the number of NSA targeting compliance incidents, expressed as a percentage of the average number of facilities tasked for acquisition during the reporting period. During this reporting period, the targeting compliance incident rate for NSA was 0.10 percent, a decrease from the prior reporting period (0.14 percent).

(U) Given that querying errors comprised a substantial number of compliance incidents during this and several prior reporting periods, this joint assessment also presents an additional metric that is designed to reflect FBI's rate of compliance with its procedures when conducting queries of unminimized Section 702-acquired information. This additional metric, the query error rate for FBI (see Figure 18, pg. 43), represents the total number of FBI query compliance incidents reported to the FISC during the reporting period, expressed as a percentage of the total number of

---

<sup>1</sup> ~~(TS//SI//NF)~~ The joint oversight team assesses that a number of factors related to the coronavirus pandemic may have contributed to a decrease in the actual number of compliance incidents during this reporting period. As one example, reduced travel during the pandemic likely resulted in fewer Section 702 targets traveling to the United States, thus reducing the likelihood that detasking delays would occur as a result of such travel. 

<sup>2</sup> (U) As explained in past joint assessments and detailed later in this current joint assessment, the overall compliance incident rate is an imperfect metric, in part because certain of the compliance incidents included in the numerator do not bear a meaningful relation to the targeting activities that form the denominator. For example, as detailed below, the number of FBI query errors is not related to the average number of facilities subject to acquisition.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

FBI queries audited by NSD<sup>3</sup> in connection with the field office reviews during which NSD identified such FBI query compliance incidents.<sup>4</sup> During this reporting period, the query error rate for FBI was 0.82 percent, a significant decrease from the prior reporting period (36.59 percent).

(U) In recent years, FBI field office reviews (which occur onsite) have been responsible for discovering a significant portion of FBI's minimization and querying incidents that are reported in each joint assessment. Because FBI field office reviews were suspended during a portion of this reporting period, incidents that might typically be discovered by NSD during those field office reviews were not discovered while the reviews were suspended.<sup>5</sup> Some of the most significant errors identified as a result of these reviews have been those related to batch queries, a functionality available in an FBI system that permits users to query multiple identifiers in sequential queries as part of a single batch job. As a result of the batch query function, a single batch job may consist entirely or largely of noncompliant queries and therefore result in thousands of improper queries; as such, the discovery of a single noncompliant batch job can substantially affect both the overall and FBI query compliance incident rates. Just a handful of non-compliant batch queries have been responsible for the wide-ranging compliance incident rates over the last several reporting periods. Whether such a noncompliant batch job involving thousands of compliance incidents would or would not have been discovered during the portion of the reporting period in which FBI field office reviews were suspended is unknown. The fact that a single noncompliant batch job can cause thousands of compliance incidents, however, may explain why even though there was only a 21.63 percent decrease in queries audited by NSD, there was a 98.22 percent decrease in FBI query incidents identified in this reporting period.<sup>6</sup> However, NSD identified query compliance issues in each field office audited during this reporting period and during calendar year 2019. And, since NSD resumed remote query reviews in 2021, NSD has continued to identify query compliance incidents in each field office audited. FBI implemented certain remedial measures in fall 2019 to address query compliance issues and, since that time, the joint oversight team has continued to work with FBI to take additional corrective actions to address the query compliance issues. The remedial measures undertaken by FBI are discussed further below.

---

<sup>3</sup> (U) ODNI only participates in a select number of FBI field office reviews. Because NSD conducts primary oversight for field office reviews, NSD will be referenced in this context throughout the report, rather than the joint oversight team.

<sup>4</sup> ~~(S//NF)~~ The number of queries audited and included in this total are queries contained in query logs provided to NSD by FBI that were run in FBI [REDACTED]. NSD has, in prior query audits, found that a small percentage of queries that were included in particular query logs were not run against unminimized FISA-acquired information, to include unminimized Section 702-acquired information.

<sup>5</sup> (U) Onsite field office reviews were suspended in March 2020, at the onset of the coronavirus pandemic and related travel restrictions in the United States. Thus, during this reporting period, NSD was conducting field office reviews for only a little more than three months. NSD resumed field office reviews remotely in February 2021, at which time NSD selected for sampling a range of historical queries conducted throughout 2020 by users in multiple FBI field offices.

<sup>6</sup> (U) FBI's minimization and querying incidents reported in this joint assessment were first reported to the FISC during this reporting period, but certain of those incidents were discovered in connection with field office reviews conducted during prior reporting periods.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~**(U) SECTION 1: INTRODUCTION**

(U) FISA Section 702(m)(1)<sup>7</sup> requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. To fulfill this requirement, a team of oversight personnel from the Department of Justice’s (DOJ) National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) (hereinafter, the “joint oversight team”) normally conducts compliance reviews to assess whether the authorities under Section 702 have been implemented in accordance with the applicable procedures and guidelines, discussed herein; however, as explained above, onsite compliance reviews during this reporting period were impacted by the coronavirus pandemic. This report sets forth NSD and ODNI’s 24<sup>th</sup> joint compliance assessment, based on regular and modified oversight activities during this reporting period, under Section 702, covering the period 01 December 2019 through 31 May 2020 (hereinafter, the “reporting period”).<sup>8</sup>

(U) Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting, minimization, and querying procedures, as well as guidelines. A primary purpose of the guidelines is to ensure compliance with the limitations set forth in subsection (b) of Section 702, which are as follows:

An acquisition authorized under subsection (a) –

- (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
- (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
- (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
- (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
- (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(U) The Attorney General’s Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter, “the Attorney General’s Acquisition Guidelines”) were adopted by the Attorney General, in consultation with the DNI, on 05 August 2008.

---

<sup>7</sup> (U) 50 U.S.C. §1881a(m)(1).

<sup>8</sup> (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702, which was previously submitted on 04 September 2020, as required by Section 707(b)(1) of FISA (hereinafter, the “Section 707 Report”). This 24<sup>th</sup> Joint Assessment covers the same reporting period as the 24<sup>th</sup> Section 707 Report.

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(h) certifications that targeted non-United States persons reasonably believed to be located outside the United States in order to acquire different types of foreign intelligence information. The foreign intelligence information must fall within a specific type (*i.e.*, category) of foreign intelligence information that has been authorized pursuant to the Section 702(h) certifications.<sup>9</sup> Four agencies are primarily involved in implementing Section 702: the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Counterterrorism Center (NCTC). An overview of how these agencies implement the authority appears in the Appendix of this assessment.

(U) Section Two of this joint assessment provides a comprehensive overview of oversight measures the Government employs to ensure compliance with the targeting, minimization, and querying procedures, as well as the Attorney General's Acquisition Guidelines. Section Three compiles and presents data acquired from the joint oversight team's compliance reviews in order to provide insight into the overall scope of the Section 702 program, as well as trends in targeting, reporting, and the minimization of United States person information. Section Four describes compliance trends. All of the specific compliance incidents for the reporting period have been previously described in detail in the corresponding Section 707 Report. As with the prior joint assessments, some of those compliance incidents are analyzed here to determine whether there are patterns or trends that might indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented processes to prevent reoccurrences. Finally, this joint assessment contains an Appendix, which as noted above, includes a general description of the oversight at each agency.

(U) As noted above, FBI had a significant number of compliance incidents related to querying of Section 702-acquired information. FBI amended its 2018 querying procedures, which were in effect for the first six days of this reporting period, in response to concerns raised by the FISC and the Foreign Intelligence Surveillance Court of Review (FISC-R) regarding the sufficiency of those procedures. The FISC ultimately determined that FBI's amended querying procedures were adequate, and the joint oversight team engaged with FBI to implement those amended procedures and provided the FISC with periodic reporting regarding that implementation. FBI's

---

9

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

query-related compliance incidents are detailed below, along with the remedial measures FBI has taken and is taking to address them.

(U) The joint oversight team finds that the agencies have continued to implement their respective procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702 during this reporting period. However, notwithstanding a focused and concerted effort by FBI personnel to comply with the requirements of Section 702, misunderstandings regarding FBI's systems and FBI's querying procedures caused a large number of query errors.

(U) In its ongoing efforts to reduce the number of future compliance incidents, the Government will continue to focus on measures to improve (a) inter- and intra-agency communication, (b) training, and (c) systems used in the handling of Section 702-acquired data, including those systems needed to ensure that appropriate purge practices are followed and that certain disseminated reports are withdrawn as required. The joint oversight team will also continue to monitor agency practices to ensure appropriate remediation steps are taken to prevent, whenever possible, reoccurrences of the types of compliance incidents discussed herein and in the Section 707 Report. Each joint assessment provides, as appropriate, updates on these on-going efforts.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~**(U) SECTION 2: OVERSIGHT OF THE IMPLEMENTATION OF SECTION 702**

(U) The implementation of Section 702 is a multi-agency effort. As described in detail in the Appendix, NSA and FBI each acquires certain types of data pursuant to their own Section 702 targeting procedures. NSA, FBI, CIA, and NCTC<sup>10</sup> each handles Section 702-acquired data in accordance with its own minimization and querying procedures.<sup>11</sup> There are differences in the way each agency implements its procedures resulting from unique provisions in the procedures themselves, differences in how these agencies utilize Section 702-acquired data, and efficiencies gained by leveraging existing agency-specific systems and processes to implement Section 702 authorities. Because of these differences in practice and procedure, there are corresponding differences in each agency's internal compliance programs and in the external NSD and ODNI oversight programs.

(U) The joint oversight team, consisting of members from NSD, the ODNI Office of Civil Liberties, Privacy, and Transparency (CLPT), the ODNI Office of General Counsel (OGC), and the ODNI Mission Integration Directorate Mission Performance, Analysis, and Collection (MPAC) Division, conducts independent Section 702 oversight activities. The team members play complementary roles in the review process. The following section describes the oversight activities of the joint oversight team, the results of which, in conjunction with the internal oversight conducted by the reviewed agencies, provide the basis for this joint assessment.

**(U) I. Joint Oversight of NSA**

(U) Under the process established by the Attorney General and DNI's certifications, all Section 702 targeting is initiated pursuant to NSA's targeting procedures. Additionally, NSA is responsible for conducting post-tasking checks of all Section 702-tasked communication facilities<sup>12</sup>

---

<sup>10</sup> (U) As discussed herein, CIA and NCTC receive Section 702-acquired data from NSA and FBI.

<sup>11</sup> (U) Each agency's Section 702 targeting, minimization, and querying procedures are approved by the Attorney General and reviewed by the FISC. The targeting, minimization, and querying procedures that were in effect during this assessment's reporting period were those approved as part of the 2018 and 2019 certifications. In October 2018, the FISC found that CIA, NCTC and NSA's querying procedures were sufficient but that FBI's querying procedures were not sufficient in certain respects. After the FISC's decision in October 2018 and a decision by the FISC-R in July 2019, the Government amended FBI's querying procedures and submitted those to the FISC in August 2019. The FISC approved the amended FBI querying procedures in September 2019. FBI's 2019 querying procedures were approved and went into effect on 06 December 2019, and were, therefore, effective for almost the entirety of this reporting period.

(U) On 08 October 2019, the DNI released, in redacted form, each of the 2018 minimization procedures and the 2018 querying procedures for NSA, FBI, CIA, and NCTC, as well the 2018 targeting procedures for NSA and FBI. On 04 September 2020, the DNI released, in redacted form, each of the 2019 minimization procedures and the 2019 querying procedures for NSA, FBI, CIA, and NCTC, as well the 2019 targeting procedures for NSA and FBI. The 2018 and 2019 procedures are posted on ODNI's *IC on the Record* website.

<sup>12</sup> (U) Section 702 authorizes the targeting of non-United States persons reasonably believed to be located outside the United States. This *targeting* is effectuated by *tasking* communication facilities (*i.e.*, selectors), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. The oversight review process, which is described in this joint assessment, applies to the tasking of every communication facility, regardless of the type of facility. A fuller description of the Section 702 targeting process may

~~TOP SECRET//SI//ORCON//NOFORN~~

(also referred to as selectors) once collection begins. NSA must also minimize its collection in accordance with its minimization procedures and must conduct queries in accordance with its querying procedures. Each of these responsibilities is detailed in the Appendix. Given its central role in the Section 702 process, NSA has devoted substantial oversight and compliance resources to monitoring its implementation of the Section 702 authorities. NSA’s internal oversight and compliance mechanisms are further described in the Appendix.

(U) NSD and ODNI’s joint oversight of NSA’s implementation of Section 702 consists of periodic compliance reviews, which NSA’s targeting procedures require,<sup>13</sup> as well as the investigation and reporting of specific compliance incidents. During this reporting period, onsite reviews were conducted at NSA on the dates shown in Figure 1.

(U) **Figure 1: NSA Reviews**

UNCLASSIFIED

Date of NSA Onsite Review	Targeting, Minimization, and Querying Reviewed
28 February 2020	01 December 2019 – 31 January 2020
19 June 2020	01 February 2020 – 31 May 2020

(U) Figure 1 is UNCLASSIFIED.

~~(S//NF)~~ Reports for each of these reviews document the relevant time period of the review, the number and types of communication facilities tasked, and the types of information that NSA relied upon, as well as provide a detailed summary of the findings for that reporting period.

[REDACTED]

[REDACTED] with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA;

[REDACTED] were provided to the congressional committees with the subsequent Section 707 report.

(U) The joint oversight review process for NSA targeting begins well before the onsite review. Prior to each onsite review, NSA electronically sends the tasking record (known as a tasking sheet) for *each* facility tasked during the reporting period to NSD and ODNI. Members of the joint oversight team initially review the tasking sheets, with ODNI team members sending any questions they may have concerning the tasking sheets to NSD, who then prepares a detailed report of the findings, including any questions and requests for additional information. NSD shares this report with the ODNI members of the joint oversight team. During this initial review, the joint oversight team determines whether the tasking sheets meet the documentation standards required by NSA’s targeting procedures and provide sufficient information to ascertain the basis for NSA’s foreignness determinations. The joint oversight team also reviews whether the tasking was in conformance with the targeting procedures and statutory requirements (*i.e.*, that the target is a non-

be found in the Appendix. This assessment uses the terms facilities and selectors interchangeably and does not make a substantive distinction between the two terms.

<sup>13</sup> (U) NSA’s targeting procedures require that the onsite reviews occur approximately every two months. Due to the coronavirus pandemic, NSD and ODNI did not conduct a planned onsite review during April 2020. Instead, the April 2020 onsite review was consolidated with the June 2020 onsite review.

~~TOP SECRET//SI//ORCON//NOFORN~~

United States person reasonably believed to be located outside the United States, and that the target is reasonably expected to possess, receive, and/or likely communicate foreign intelligence information related to the categories of foreign intelligence information specified in the certifications). For those tasking sheets that, on their face, meet the standards and provide sufficient information, no further supporting documentation is requested. The joint oversight team then identifies the tasking sheets that did not provide sufficient information and requests additional information.

(U) During the onsite review, the joint oversight team examines the cited documentation underlying these identified tasking sheets, together with NSA's Office of Compliance for Cyber and Operations (OCCO), NSA attorneys, and other NSA personnel, as required. The joint oversight team works with NSA to answer questions, identify issues, clarify ambiguous entries, and provide guidance on areas of potential improvement. Interaction continues following the onsite reviews in the form of electronic and telephonic exchanges to answer questions and clarify issues.

(U) The joint oversight team also reviews NSA's minimization of Section 702-acquired data. NSD currently reviews all of the serialized reports (ODNI reviews a sample) that NSA has disseminated and identified as containing Section 702-acquired United States person information. The team also reviews a sample of serialized reports that NSA has disseminated and identified as containing Section-702 acquired *non*-United States person information. NSD and ODNI also review a sample of NSA disseminations to certain foreign government partners made outside of its serialized reporting process. These disseminations consist of information that NSA has evaluated for foreign intelligence and minimized, but which may not have been translated into English.

(U) NSA's Section 702 querying procedures provide that any use of United States person identifiers as terms to identify and select Section 702-acquired data must be accompanied by a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information, as defined in FISA. With respect to queries of Section 702-acquired *content* using a United States person identifier, the procedures provide that the United States person identifier must first be approved by NSA's OGC. The joint oversight team reviews all approved United States person identifiers to ensure compliance with NSA's querying procedures.<sup>14</sup> For each approved identifier, NSA also provides information detailing why the proposed use of the United States person identifier would be reasonably likely to return foreign intelligence information, the date that the United States person identifier was authorized to be used

---

<sup>14</sup> (U) On 30 April 2020, the DNI publicly released ODNI's seventh annual Transparency Report[s]: *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2019* (hereinafter, the "CY2019 Transparency Report"). Pursuant to reporting requirements proscribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(B)), the 2019 Transparency Report provided the "estimated number of search terms concerning a known United States person used to retrieve the unminimized contents of communications obtained under Section 702" (emphasis added) for the entire calendar year of 2019. The CY2019 Transparency Report only covers one month during this assessment's reporting period (December 2019 through May 2020). Subsequently, the DNI publicly released the CY2020 Transparency Report on 30 April 2021; the CY2020 Transparency Report covers the remaining months of this assessment's reporting period.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

as a query term,<sup>15</sup> and any other relevant information. In addition, with respect to queries of Section 702-acquired *metadata* using a United States person identifier, NSA's querying procedures require that NSA analysts document the basis for each such metadata query prior to conducting the query. NSD reviews the documentation for 100 percent of such metadata queries that NSA provides to NSD.<sup>16</sup>

(U) Additionally, the joint oversight team investigates and reports incidents of noncompliance with NSA's targeting, minimization, and querying procedures, as well as with the Attorney General Acquisition Guidelines. While some of these incidents may be identified during the reviews, most are identified by NSA analysts or by NSA's internal compliance program. NSA is also required to report certain events that may not be incidents of non-compliance. For example, NSA is required to report *all* instances in which Section 702 acquisition continued while a targeted individual was in the United States, whether or not NSA had any knowledge of the target's travel to the United States.<sup>17</sup> The purpose of such reporting is to allow the joint oversight team to assess whether a compliance incident has occurred and to confirm that any necessary remedial action is taken. Investigations of these incidents sometimes result in requests for supplemental information. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

## (U) II. Joint Oversight of FBI

(U) FBI fulfills various roles in the implementation of Section 702, which are set forth in further detail in the Appendix. First, FBI is authorized under the certifications to acquire foreign intelligence information. Those acquisitions must be conducted pursuant to FBI's Section 702 targeting procedures.

~~(S//NF)~~ Second, FBI also

Pursuant to its own authority, FBI is authorized to from electronic communication service providers by targeting facilities that NSA

<sup>15</sup> (U) NSA's Section 702 querying procedures provide that NSA may approve the use of a United States person identifier to query Section 702-acquired *content* for no longer than a period of one year and that such approvals may be renewed for periods up to one year.

<sup>16</sup> (U) Also pursuant to reporting requirements prescribed by the USA FREEDOM Act (*see* 50 U.S.C. § 1873(b)(2)(C)), the CY2019 Transparency Report provided the "estimated number of queries concerning a known United States person used to retrieve the unminimized noncontents [(i.e., metadata)] information obtained under Section 702" (emphasis added) for the entire calendar year of 2019. The same statistics were provided in the CY2020 Transparency Report.

<sup>17</sup> (U) If NSA had no prior knowledge of the target's travel to the United States and, upon learning of the target's travel, "detasked" (i.e., stopped collection against) the target's facility without delay, as is required by NSA's targeting procedures, the collection while the target was in the United States would not be considered a compliance incident under NSA's targeting procedures, although the collection would generally be subject to purge under the applicable minimization procedures. The joint oversight team carefully considers, and where appropriate, obtains additional facts regarding every reported detasking decision to ensure that NSA's tasking and detasking complied with its targeting procedures.

~~TOP SECRET//SI//ORCON/NOFORN~~

designates (hereinafter, “Designated Accounts”). FBI conveys [REDACTED] from the electronic communications service providers [REDACTED] for processing in accordance with the agencies’ FISC-approved minimization procedures.

~~(S//NF)~~ Third, FBI may receive [REDACTED]<sup>8</sup> unminimized Section 702-acquired communications. Such communications must be minimized pursuant to FBI’s Section 702 minimization procedures. As described below, FBI has a process for nominating to NSA new facilities to be targeted pursuant to Section 702.

~~(S//NF)~~ NSD and ODNI’s oversight program is designed to ensure FBI’s compliance with statutory and procedural requirements for each of those three roles. The joint oversight team generally conducts monthly reviews at FBI headquarters of FBI’s compliance with its targeting procedures and quarterly reviews at FBI headquarters of FBI’s compliance with its minimization procedures. However, due to the coronavirus pandemic, the joint oversight team did not conduct onsite reviews at FBI headquarters after mid-March 2020. Instead, the joint oversight team conducted reviews of FBI’s application of its targeting and minimization procedures remotely. As a result of FBI’s reduced staffing due to the coronavirus pandemic, FBI was unable to gather the information necessary to finalize two of the reports before the production to Congress of the Section 707 Report; the remaining reports were subsequently finalized with the help of FBI and were provided to the congressional committees with subsequent Section 707 reports. For this reporting period, reviews were conducted during the dates shown in Figure 2.

**(U) Figure 2: FBI Reviews**

UNCLASSIFIED

Approximate Date of FBI Review	Targeting and Minimization Reviewed
04 and 05 February 2020 (onsite)	December 2019 targeting decisions
April 2020 (remote)	January 2020 targeting decisions
June 2020 (remote)	February and March 2020 targeting decisions; 01 December 2019 – 31 May 2020 minimization decisions
August 2020 (remote)	April and May 2020 targeting decisions

(U) Figure 2 is UNCLASSIFIED.

(U) In conducting targeting reviews, the joint oversight team reviews the targeting checklists completed by FBI analysts and supervisory personnel involved in the process, together with supporting documentation.<sup>19</sup> The joint oversight team also reviews a sample of other files to identify any other potential compliance issues. FBI analysts, supervisory personnel, and attorneys

<sup>18</sup> [REDACTED]

<sup>19</sup> ~~(S//NF)~~ If FBI’s application of its targeting procedures to [REDACTED] returns information from the databases discussed in FBI’s targeting procedures, then FBI provides a checklist that shows the results of its database queries. If FBI’s database queries returned results that FBI identifies as relevant to the target’s location or citizenship status, then FBI also provides the joint oversight team with supporting documentation. [REDACTED]

[REDACTED] During this reporting period, the joint oversight team reviewed a sample of checklists and supporting documentation provided by FBI for approved requests for which information is returned by FBI’s database queries.

~~TOP SECRET//SI//ORCON//NOFORN~~

from FBI's National Security and Cyber Law Branch (NSCLB) are available to answer questions and provide supporting documentation. The joint oversight team provides guidance on areas of potential improvement.

(U) In conducting FBI minimization reviews, the joint oversight team reviews documents related to FBI's application of its Section 702 minimization procedures. The team reviews a sample of communications that FBI has marked in its systems as both meeting the retention standards and containing United States person information. The team also reviews all disseminations by the relevant FBI headquarters unit of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States persons.

(U) During a portion of this reporting period, NSD conducted minimization and querying reviews at FBI field offices in order to review the retention, querying, and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. NSD did not conduct any reviews at FBI field offices in April or May 2020 because it suspended its onsite reviews in March 2020 in response to the coronavirus pandemic. Subsequent to this reporting period, in February 2021, NSD resumed conducting remote reviews of queries of unminimized FISA collection conducted by some FBI field offices. In the reviews conducted prior to the pandemic, NSD reviewed a sample of retention decisions made by FBI personnel in connection with investigations involving the acquisition of data pursuant to Section 702 and a sample of disseminations of information acquired pursuant to Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States persons. NSD also reviewed a sample of queries by FBI personnel in FBI systems that contain unminimized FISA-acquired information, including Section 702-acquired information. Those reviews evaluate whether the queries complied with the requirements in FBI's FISA minimization and querying procedures, including its Section 702 querying procedures. In addition, as a result of a Court-ordered reporting requirement first set forth in the FISC's *November 6, 2015 Memorandum Opinion and Order*<sup>20</sup> for queries conducted after 4 December 2015, as well as certain requirements in the FISA statute, NSD reviews those queries to determine if any such queries were conducted solely for the purpose of returning evidence of a crime. If such a query was conducted, NSD would seek additional information as to whether FBI personnel received and reviewed Section 702-acquired information of or concerning a United States person in response to such a query. Pursuant to the FISC's opinion and order, such queries must subsequently be reported to the FISC.

(U) As detailed in the attachments to the Attorney General's Section 707 Report, NSD conducted minimization and querying reviews at seven FBI field offices during this reporting period

---

<sup>20</sup> (U) The FISC's 6 November 2015 Opinion and Order approved the 2015 FISA Section 702 Certifications. On 19 April 2016, the DNI, in consultation with the Attorney General, released in redacted form, this *Opinion and Order* on the ODNI public website *IC on the Record*. This Court-ordered reporting requirement was carried forward in subsequent Section 702 FISC opinions.

(S//NF) The title of the FISC's 6 November 6 2015 opinion is [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

and reviewed cases involving Section 702-tasked facilities.<sup>21</sup> ODNI received written summaries regarding all of the reviews from NSD. Those reviews are further discussed in Section IV below.

~~(S//NF)~~ Separately, in order to evaluate FBI [REDACTED] acquisition [REDACTED] and provision of [REDACTED] the joint oversight team conducts an annual process review with FBI's technical personnel to ensure that those activities complied with applicable minimization procedures. While outside this reporting period, the most recent annual process review occurred in June 2021.

~~(S//NF)~~ As further described in detail in the Appendix, FBI nominates potential Section 702 [REDACTED]

[REDACTED] FBI has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Those processes are further described in the Appendix.

(U) Throughout the reporting period, the joint oversight team also investigates potential incidents of noncompliance with FBI's targeting, minimization, and querying procedures, the Attorney General's Acquisition Guidelines, or other agencies' procedures in which FBI is involved.<sup>22</sup> Those investigations are coordinated with FBI's Office of General Counsel (OGC) and may involve requests for further information; meetings with FBI legal, analytical, and/or technical personnel; or review of source documentation. Compliance incidents identified by those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

### (U) III. Joint Oversight of CIA

(U) As further described in detail in the Appendix, although CIA does not directly engage in targeting or acquisition, it does nominate potential Section 702 targets to NSA. Because CIA nominates potential Section 702 targets to NSA, the joint oversight team typically conducts onsite visits at CIA,<sup>23</sup> and includes the results of those visits in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities.

---

<sup>21</sup> ~~(S//NF)~~ During those field office reviews, NSD reviewed [REDACTED] cases involving Section 702-tasked facilities.

<sup>22</sup> (U) Insofar as FBI nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with NSA's targeting procedures can also involve FBI.

<sup>23</sup> (U) Due to the coronavirus pandemic, the joint oversight team did not conduct onsite reviews at CIA during this reporting period. Instead, the joint oversight team conducted reviews of CIA's application of its minimization and querying procedures remotely over a period of several weeks.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

(U) The reviews also focus on CIA's application of its Section 702 minimization procedures and querying procedures.<sup>24</sup> Reports for each of those reviews have previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA. For this reporting period, the joint oversight team conducted reviews of CIA's application of its minimization and querying procedures during the dates shown in Figure 3.

(U) **Figure 3: CIA Reviews**

UNCLASSIFIED

Approximate Dates of CIA Review	Minimization and Querying Reviewed
April – July 2020	01 December 2019 – 31 January 2020
July – August 2020	01 February 2020 – 31 March 2020
July – August 2020	01 April 2020 – 31 May 2020

(U) Figure 3 is UNCLASSIFIED.

(U) As a part of the typical onsite reviews, the joint oversight team examines documents related to CIA's retention, dissemination, and querying of Section 702-acquired data. The team reviews a sample of communications acquired under Section 702 and identified as containing United States person information that have been minimized and retained by CIA. Reviewers ensure that communications have been properly minimized and discuss with CIA personnel issues involving the proper application of CIA's minimization procedures. The team also reviews all disseminations of information acquired under Section 702 that CIA identified as potentially containing United States person information.<sup>25</sup> In addition, NSD reviews CIA's written foreign intelligence justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications to assess whether those queries were compliant with CIA's querying procedure requirements that such queries are reasonably likely to return foreign intelligence information, as defined by FISA.

~~(S//NF)~~ CIA may receive [REDACTED] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to CIA's minimization procedures. Additionally, and as further described in detail in the Appendix, CIA nominates potential Section 702 targets to NSA. [REDACTED]

[REDACTED] the joint oversight team conducts onsite visits at CIA to review CIA's original source documentation [REDACTED] the results of those visits are included in the bimonthly NSA review reports discussed previously. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. Those processes are further described in the Appendix.

<sup>24</sup> (U) The query requirements for CIA that were in effect during this reporting period are contained in CIA's Section 702 querying procedures for the 2018 and 2019 Certifications, which were posted on *IC on the Record* on 08 October 2019, and 04 September 2020, respectively.

(U) <sup>25</sup> ~~(S//NF)~~ Due to the sensitive nature of these disseminations, they must be reviewed in person at CIA. On 23 March 2021, and 24 March 2021, representatives from NSD and ODNI conducted an onsite review at CIA of the disseminations from this reporting period.

~~TOP SECRET//SI//ORCON/NOFORN~~

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with CIA’s minimization and querying procedures, the Attorney General Acquisition Guidelines, or other agencies’ procedures in which CIA is involved.<sup>26</sup> Investigations are coordinated through CIA’s FISA Program Office and CIA’s Office of General Counsel (CIA OGC), and when necessary, may involve requests for further information, meetings with CIA legal, analytical and/or technical personnel, or the review of source documentation. All compliance incidents identified by those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

**(U) IV. Joint Oversight of NCTC**

~~(S//NF)~~ NCTC is authorized to receive unminimized Section 702 information and also has access to certain FBI systems containing minimized Section 702 information pertaining to counterterrorism. NCTC’s processing, retention, and dissemination of such information is subject to its Section 702 minimization procedures. Unlike NSA, FBI, and CIA, NCTC does not directly engage in targeting or acquisition, nor does it nominate potential Section 702 targets to NSA. NCTC may receive [REDACTED] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to NCTC’s minimization procedures. NCTC has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. As part of the joint oversight of NCTC’s access, receipt, and processing of unminimized Section 702 information and minimized Section 702 information from FBI, the joint oversight team typically conducts onsite visits at NCTC, and the results of those visits are included in bimonthly NCTC review reports. However, due to the coronavirus pandemic, the joint oversight team conducted only one onsite review at NCTC during the review period. NSD and ODNI conducted the other two bimonthly reviews during the review period remotely.

(U) The reviews focus on NCTC’s application of its Section 702 minimization procedures and querying procedures. Reports for each of those reviews have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA. For this reporting period, reviews of NCTC’s application of its minimization and querying procedures were conducted on the dates shown in Figure 4.

**(U) Figure 4: NCTC Reviews**

UNCLASSIFIED

Approximate Date of NCTC Review	Minimization and Querying Reviewed
23 January 2020 (onsite)	01 November 2019 – 31 December 2019
March 2020 (remote)	01 January 2020 – 29 February 2020
May 2020 (remote)	01 March 2020 – 30 April 2020

(U) Figure 4 is UNCLASSIFIED.

(U) As a part of the reviews, the joint oversight team examines documents related to NCTC’s retention, dissemination, and querying of Section 702-acquired data. The team reviews all

<sup>26</sup> (U) Insofar as CIA nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible non-compliance with NSA’s targeting procedures can also involve CIA.

~~TOP SECRET//SI//ORCON//NOFORN~~

communications acquired under Section 702 that have been minimized and retained by NCTC, irrespective of whether it contains United States person information. Reviewers ensure that communications have been properly minimized and discuss with personnel issues involving the proper application of NCTC's minimization procedures. The team also reviews all NCTC disseminations of information acquired under Section 702. In addition, the joint oversight team reviews NCTC's written foreign intelligence justifications for all queries of the content of unminimized Section 702-acquired communications.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with NCTC's minimization and querying procedures or other agencies' procedures in which NCTC is involved.<sup>27</sup> Investigations are coordinated through the NCTC Compliance and Transparency Group and NCTC Legal, a forward deployed component of the ODNI OGC, and when necessary, may involve requests for further information; meetings with NCTC legal, analytical, and/or technical personnel; or the review of source documentation. All compliance incidents identified by those investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(U) **V. Interagency / Programmatic Oversight**

(U) Because the implementation and oversight of the Government's Section 702 authorities are multi-agency efforts, investigations of particular compliance incidents may involve more than one agency. The resolution of particular compliance incidents can provide lessons learned for all agencies. Robust communication among the agencies is required for each to effectively implement its authorities, gather foreign intelligence information, and comply with all legal requirements. For those reasons, NSD and ODNI generally lead calls and meetings on relevant compliance topics, including calls or meetings with representatives from all agencies implementing Section 702 authorities, so as to address interagency issues affecting compliance with the statute and applicable procedures. Additionally, during a portion of this reporting period, NSD and ODNI conducted weekly telephone calls with NSA to address certain outstanding compliance matters and work through the process of understanding those matters and reporting incidents to the FISC.

(U) NSD and ODNI's programmatic oversight also involves efforts to proactively minimize the number of incidents of noncompliance. For example, NSD and ODNI have required agencies to provide a demonstration to the joint oversight team of new or substantially revised systems involved in Section 702 targeting, minimization, or querying prior to implementation. NSD and ODNI personnel also continue to work with the agencies to review and, where appropriate, seek modifications of their targeting, minimization, and querying procedures in an effort to enhance the Government's collection of foreign intelligence information, civil liberties protections, and compliance.

---

<sup>27</sup> (U) Insofar as NCTC reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with NSA's targeting procedures can also involve NCTC.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~**(U) VI. Training**

(U) In addition to specific instructions to personnel directly involved in certain incidents of noncompliance discussed in Section 4, the agencies and the joint oversight team have continued their training efforts to ensure compliance with the targeting, minimization, and querying procedures. During this reporting period, NSA continued to administer the compliance training course dated November 2016.<sup>28</sup> All NSA personnel who require access to Section 702 data are required to complete this course on an annual basis in order to gain or maintain that access. Additionally, NSA continued providing training on a more informal and ad hoc basis by issuing training reminders and compliance advisories to analysts concerning new or updated guidance to maintain compliance with the Section 702 procedures. Those training reminders and compliance advisories are e-mailed to individual analysts and targeting adjudicators and maintained on internal agency websites<sup>29</sup> where personnel can obtain information about specific types of Section 702-related issues and compliance matters.

(U) During this reporting period, FBI similarly continued implementing its online training programs regarding Section 702 nominations, minimization, and other related requirements; however, in March 2020, the in-person training was suspended due to the pandemic. Completion of those FBI online training programs is required of all FBI personnel who request access to Section 702 information. NSD and FBI also conducted in-person trainings at multiple FBI field offices. For example, during this reporting period, prior to March 2020, NSD and FBI continued to provide additional focused training at FBI field offices on the Section 702 querying procedures, including training FBI field personnel on the application of the querying standard. NSD training at FBI field offices also included training on the reporting requirement from the FISC's *November 6, 2015 Memorandum Opinion and Order* regarding the 2015 FISA Section 702 Certifications. As discussed above, this reporting requirement applies to queries conducted after 04 December 2015, which were conducted solely for the purpose of returning evidence of a crime and returned Section 702-acquired information of or concerning a United States person that was reviewed by FBI personnel.

(U) As part of its efforts to address certain issues causing the large number of non-compliant queries, in June 2018, and in November 2019, FBI worked with NSD and ODNI to develop updated guidance on the query provisions in FBI's procedures. This enhanced training on the query restrictions in FBI's procedures was designed to address misunderstandings regarding the query standard and how to avoid non-compliant queries. More recently, FBI developed training focused on the query provisions in its Section 702 querying procedures, including system changes designed

---

<sup>28</sup> (U) NSA released the transcript associated with this training, dated August 2016, in response to a Freedom of Information Act (FOIA) case filed in the U.S. District Court, Southern District of New York, ACLU v. National Security Agency, et al. (hereinafter, the "ACLU FOIA"). The transcript was posted, in redacted form, on ODNI's *IC on the Record* on 22 August 2017. The transcript is titled, *OVSC1203: FISA Amendments Act Section 702* (Document 17, NSA's Training on FISA Amendments Act Section 702). The November 2016 training is in the process of being revised, with an expected rollout in 2022.

<sup>29</sup> (U) These documents were posted, in redacted form, on ODNI's *IC on the Record* on 23 August 2017, in response to the aforementioned ACLU FOIA case: *NSA's 702 Targeting Review Guidance* (Document 10), *NSA's 702 Practical Applications Training* (Document 11), *NSA's 702 Training for NSA Adjudicators* (Document 12), and *NSA's 702 Adjudication Checklist* (Document 13).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

to address aspects of the 2018 amended querying procedures. This training was mandatory for FBI personnel who are authorized to access unminimized Section 702-acquired information. FBI conducted this training between November and December 2019. Users who did not complete this training by mid-December 2019 had their access to unminimized Section 702-acquired information temporarily suspended until they took the training.

(U) During this reporting period, CIA provided targeted FISA training to attorneys it embeds with CIA operational personnel who regularly address FISA matters, and continued to provide FISA training to any attorney beginning an assignment that may involve the provision of legal advice on FISA matters. Additionally, CIA has a required training program for anyone handling unminimized Section 702-acquired data that provides hands-on experience with handling and minimizing Section 702-acquired data, as well as the Section 702 nomination process; during this reporting period, CIA continued to implement this training, which is required for all personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Furthermore, CIA has issued guidance to its personnel about how to properly conduct United States person queries that are reasonably likely to return foreign intelligence information.<sup>30</sup>

(U) During this reporting period, NCTC provided training on NCTC's Section 702 minimization and querying procedures to all of its personnel who will have access to unminimized Section 702-acquired information. NCTC uses a training tracking system through which NCTC can verify that its users have received the appropriate Section 702 training before being given access to unminimized Section 702-acquired information. In addition, NCTC conducts audits of personnel at NCTC who accessed unminimized Section 702-acquired information in its system to confirm that those personnel who access unminimized Section 702-acquired information have received training on NCTC's Section 702 minimization and querying procedures.

---

<sup>30</sup> (U) See *USP Query Guidance for Personnel with Access to Unminimized FISA Section 702 Data*. As discussed in the previous joint assessment, in response to the aforementioned ACLU FOIA case, CIA's guidance document was posted, in redacted form, on ODNI's *IC on the Record* on 11 April 2017, see Document 15 "CIA's United States Person Query Guidelines for Personnel."

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(U) **SECTION 3: TRENDS IN SECTION 702  
TARGETING AND MINIMIZATION**

(U) In conducting the above-described oversight program, NSD, ODNI, and the agencies have collected a substantial amount of data regarding the implementation of Section 702. In this section, a comprehensive collection of this data has been compiled in order to identify overall trends in the agencies' targeting, minimization, and compliance.

~~(S//NF)~~ (U) This reporting period was disrupted by the coronavirus pandemic. This section and Section 4 report trends compared with the previous reporting period. The joint assessment team believes many of the changes during this reporting period, as compared to previous reporting periods, are attributable, at least in part, [REDACTED]

(U) **I. Trends in NSA Targeting and Minimization**

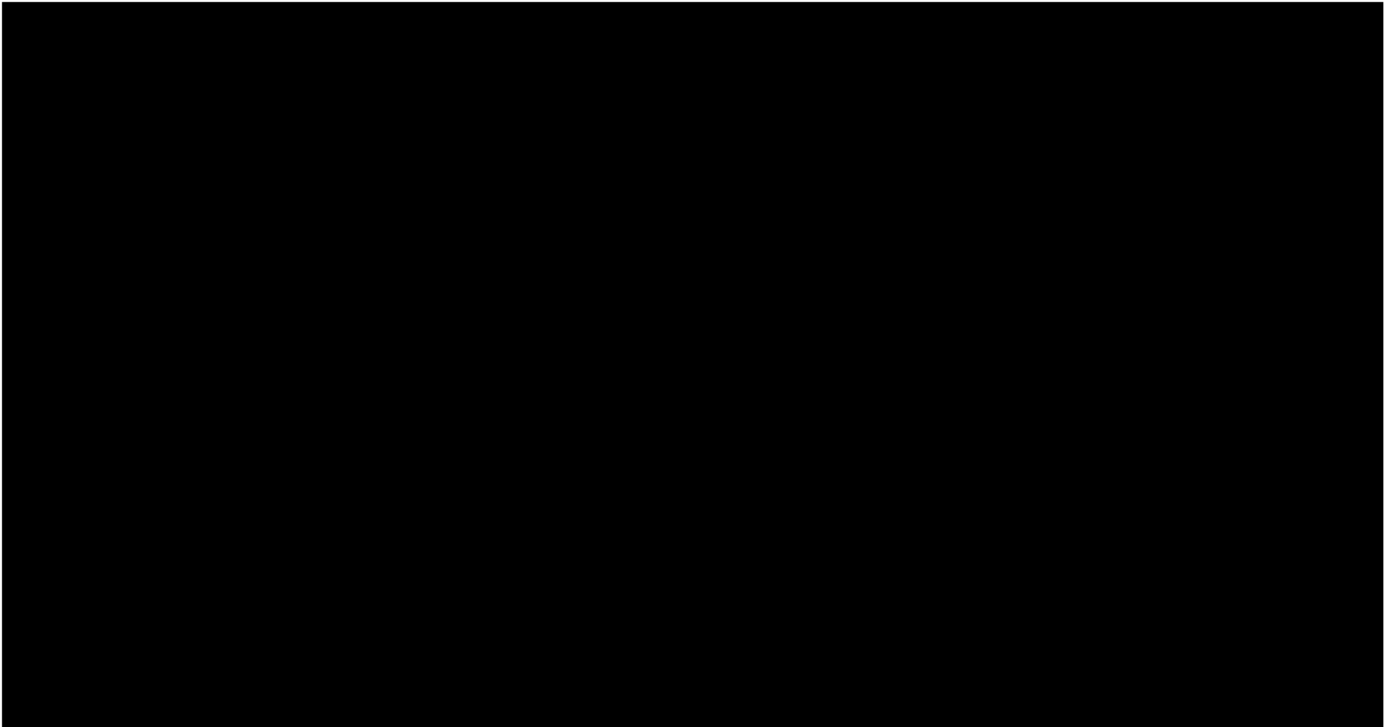
(U) NSA provides to the joint oversight team the average approximate number of facilities that were under collection on any given day during the reporting period. Because the actual number of facilities tasked remains classified,<sup>31</sup> the figure charting the average number of facilities under collection is classified as well. Since the inception of the program, the total number of facilities under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced minor decreases.<sup>32</sup>

---

<sup>31</sup> (U) The provided number of facilities, on average, subject to acquisition during the reporting period remains classified and is different from the unclassified estimated number of targets affected by Section 702 released by the ODNI in its *CY2019 Transparency Report and CY2020 Transparency Report*. The classified numbers estimate the number of *facilities* subject to Section 702 acquisition, whereas the unclassified numbers provided in the Transparency Report estimate the number of Section 702 *targets*. As noted in the Transparency Report, the number of 702 "targets" reflects an estimate of the number of known users of particular facilities, subject to intelligence collection under those Certifications. The classified number of facilities account for those facilities subject to Section 702 acquisition *during the current six month reporting period*, whereas the Transparency Report estimates the number of targets affected by Section 702 *during the calendar year*.

<sup>32</sup> (U) Both reporting periods in which the total number of facilities under collection decreased occurred prior to the reporting periods reflected in Figure 5.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~**(U) Figure 5: Average Number of Facilities under Collection**

(U) Figure 5 is classified ~~SECRET~~ [REDACTED]

~~(TS//SI//NF)~~ NSA reports that, on average, approximately [REDACTED] facilities<sup>33</sup> were under collection pursuant to the applicable certifications on any given day during the reporting period. This represents a 9.5 percent increase from the approximately [REDACTED] facilities under collection on any given day in the last reporting period. The 9.5 percent increase is relatively low compared with recent reporting periods; over the previous five reporting periods, the percentage increase ranged from 15.4 percent to 24.4 percent. [REDACTED]

<sup>33</sup> ~~(TS//SI//NF)~~ The Government counts the tasking of [REDACTED] to ensure consistency with how it counts other tasked facilities. Depending on the number [REDACTED] in a given reporting period, counting [REDACTED] could potentially skew the numbers and percentages in such a way that the statistics provided would no longer function as a barometer for the overall health of the Section 702 program.

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]

(U) The above statistics describe the *average* number of facilities under collection at any given time during the reporting period. The total number of *newly* tasked facilities during the reporting period provides another useful metric.<sup>34</sup> Figure 6 charts the average monthly numbers of newly tasked facilities from 2015 through November 2019 and the total monthly numbers of newly tasked facilities from December 2019 through May 2020.

(U) **Figure 6: New Taskings by Month (Yearly Average for 2015 through November 2019)**

[REDACTED]

(U) Figure 6 is classified ~~SECRET~~ [REDACTED]

~~(S//SI//NF)~~ NSA provided documentation of approximately [REDACTED] new taskings during the reporting period. As noted elsewhere in this report, the decline from the [REDACTED] taskings reported for the previous reporting period [REDACTED]. As shown in Figure 6, the number of new taskings in April and May fell substantially to approximately 2016 tasking levels. Unlike the last several reporting periods, the increase in the number of newly tasked facilities from December 2019 through March 2020 was largely driven by increases in the number of tasked electronic communication accounts. From June 2019 through November 2019, NSA tasked an average of approximately [REDACTED] electronic communication accounts per month. From December 2019 through March 2020, NSA tasked an average of approximately [REDACTED] electronic

<sup>34</sup> (U) The term “newly tasked facilities” refers to any facility that was added to collection under a certification. This term includes any facility added to collection pursuant to the Section 702 targeting procedures; some of these newly tasked facilities are facilities that had been previously tasked for collection, were detasked, and were then retasked.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

communication accounts per month – an increase of approximately [REDACTED] taskings per month. In comparison, over the same time period, telephony facilities only increased by an average of approximately [REDACTED] taskings per month.

(U) With respect to minimization, NSA identified to the joint oversight team the number of serialized reports NSA generated based upon minimized Section 702-acquired data and provided NSD and ODNI access to all reports NSA identified as containing United States person information. Figure 7 contains the classified number of serialized reports and reports identified as containing United States person information over the last 10 reporting periods. The NSD and ODNI reviews revealed that the United States person information was at least initially masked in the vast majority of circumstances.<sup>35</sup> The number of serialized reports NSA has identified as containing United States person information decreased when compared with the previous reporting period.

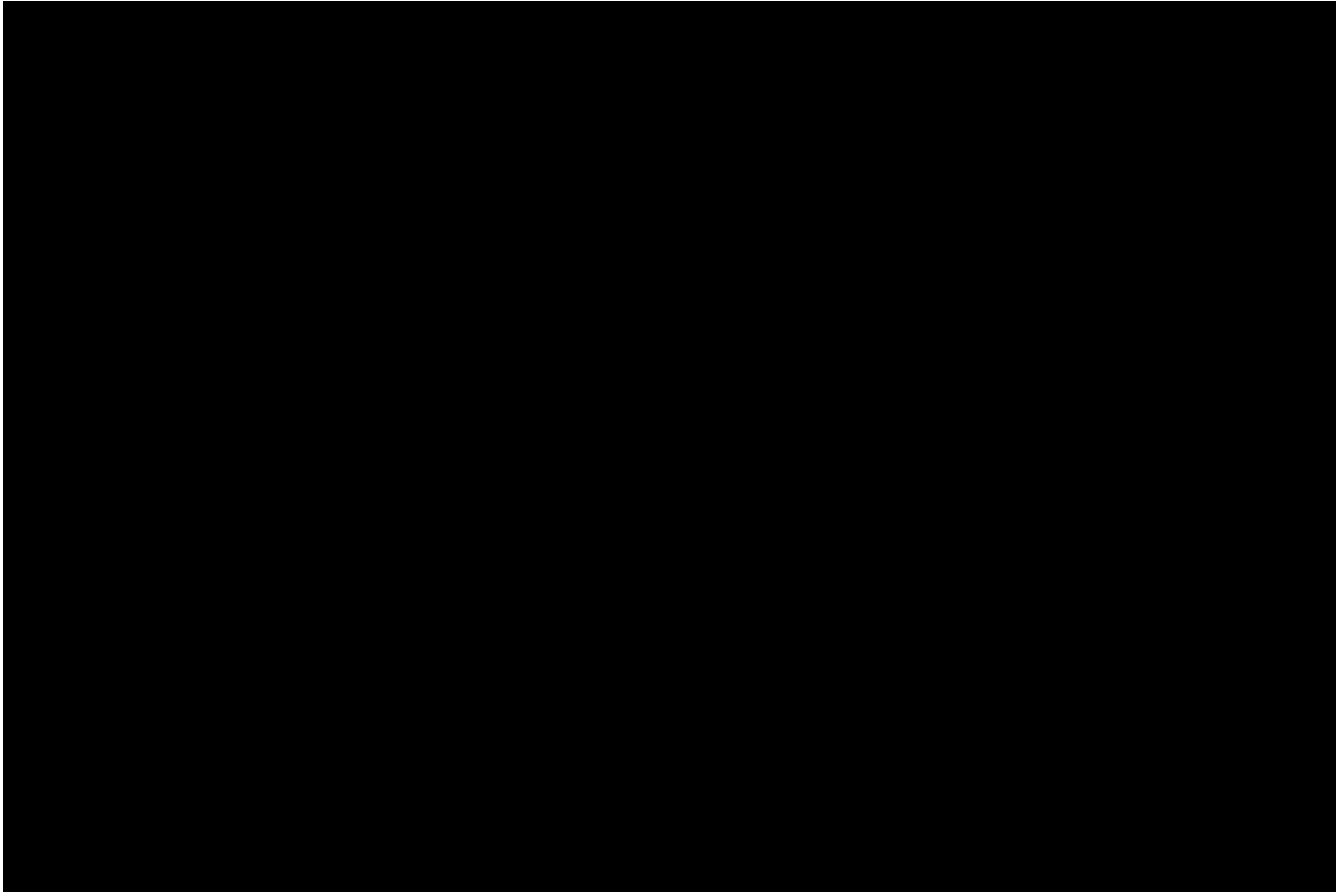
---

<sup>35</sup> (U) NSA generally “masks” United States person information by replacing the name or other identifying information of the United States person with a generic term, such as “United States person #1.” Agencies may request that NSA “unmask” the United States person identity. Prior to such unmasking, NSA must determine that the United States person’s identity meets the applicable standards in NSA’s minimization procedures.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

**(U) Figure 7: Total Disseminated NSA Serialized Reports Based Upon Section 702-Acquired Data and Number of Such Reports NSA Identified as Containing United States Person Information<sup>36</sup>**



(U) Figure 7 is classified ~~SECRET//NOFORN~~.

~~(S//NF)~~ For this reporting period NSA identified to NSD and ODNI approximately [REDACTED] serialized reports based upon minimized Section 702-acquired data. The number of serialized reports identified as containing United States person information decreased from [REDACTED] in the prior reporting period, to the current [REDACTED].<sup>37</sup>

---

<sup>36</sup> ~~(S//NF)~~ In the course of preparing this report, NSD and ODNI identified a formatting error that resulted in the incorrect reporting of the number of NSA reports identified as containing United States person information for June 1, 2017 through November 30, 2017 in the prior joint assessment. The correct number is [REDACTED].

<sup>37</sup> (U) NSA does not maintain records that allow it to readily determine, in the case of a report that includes information from several sources, from which source a reference to a United States person was derived. Accordingly, the references to United States person identities may have resulted from collection pursuant to Section 702 or from other authorized signals intelligence activity conducted by NSA that was reported in conjunction with information acquired under Section 702. Thus, the number provided above is assessed to likely be over-inclusive. NSA has previously provided this explanation in its Annual Review pursuant to Section 702(l)(3) that is provided to Congress.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(U) **II. Trends in FBI Targeting**

(U) Under Section 702, NSA designates and submits facilities to FBI for acquisition of communications from certain facilities (hereinafter, “Designated Accounts”) that have been previously approved for Section 702 acquisition under NSA’s targeting procedures. FBI applies its own targeting procedures with regard to these Designated Accounts. FBI reports to the joint oversight team the specific number of facilities designated by NSA and the number of such Designated Accounts.<sup>38</sup> As detailed below, the number of Designated Accounts decreased from the prior reporting period, which may be due, at least in part, to the coronavirus pandemic.<sup>39</sup>

(U) As Figure 8 details, FBI approves the vast majority of Designated Accounts and the percentage of approved Designated Accounts has been consistently high across reporting periods. The high level of approval can be attributed to the fact that the Designated Accounts have already been evaluated and found to meet NSA’s targeting procedures. FBI may not approve NSA’s request for acquisition of a Designated Account for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the Designated Account are non-United States persons located outside the United States. Historically, the joint oversight team notes that for those accounts not approved by FBI, only a small portion<sup>40</sup> were rejected on the basis that they were ineligible for Section 702 collection.

(U) The yearly average of Designated Accounts approved by FBI increased each year from 2015 through November 2019. The number of Designated Accounts approved by FBI each month in this reporting period has varied. NSD and ODNI have continued to track the number of Designated Accounts approved by FBI and will incorporate this information into future joint assessments.

---

~~(S//NF)~~ Outside of this reporting period, NSA identified that a technical error caused it to not identify for NSD and ODNI approximately [REDACTED] serialized reports as containing United States person information. The [REDACTED] serialized reports are included in the [REDACTED] figure.

38


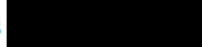




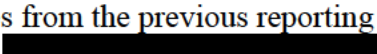


39

40

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~~~(S//NF)~~ Figure 8: 

(U) Figure 8 is classified ~~SECRET//NOFORN~~.

~~(S//SI//NF)~~ FBI reports that NSA designated approximately  accounts  during the reporting period – an average of approximately  Designated Accounts per month.<sup>41</sup> FBI approved approximately <sup>42</sup> requests . These are decreases from the previous reporting period in which NSA designated approximately  accounts  and FBI approved approximately  requests. Figure 8 shows that both numbers declined substantially in April and May 2020, likely due, at least in part, to the pandemic. In addition, Figure 8 illustrates that in these same months FBI approved more requests .

<sup>41</sup> 

(U)<sup>42</sup> ~~(S//NF)~~ As previously noted, beginning with the joint assessment covering the reporting period December 2017 through May 2018, the Government changed its counting methodology to ensure statistical accuracy for the number of Designated Accounts approved.

~~TOP SECRET//SI//ORCON/NOFORN~~

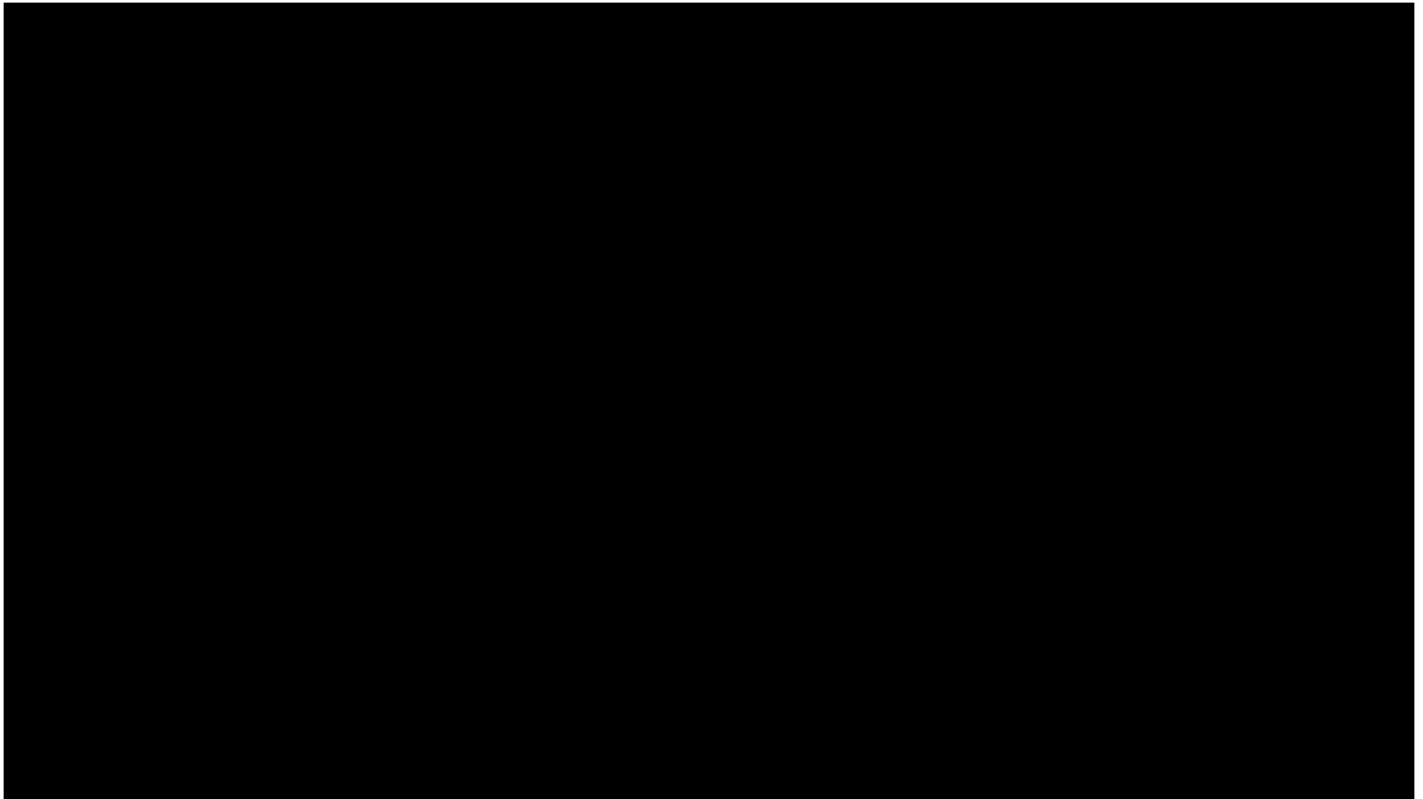
~~TOP SECRET//SI//ORCON/NOFORN~~

█ than the number of accounts designated by NSA; this reflects FBI's continued processing of requests submitted by NSA in prior months.

(U) **III. Trends in CIA Minimization**

(U) CIA only identifies for NSD and ODNI disseminations of Section 702-acquired United States person information. Figure 9 compiles the number of such disseminations of reports containing United States person information identified in the last 10 reporting periods (June 2015 through November 2015 through the current period of December 2019 through May 2020). While the number of CIA-identified disseminations containing United States person information has fluctuated over the years, those fluctuations have generally been incremental whether upward or downward.

(U) **Figure 9: Disseminations Identified by CIA as Containing Minimized Section 702-Acquired United States Person Information (Excluding Certain Disseminations to NCTC)**



(U) Figure 9 is classified ~~SECRET//NOFORN~~.

~~(S//NF)~~ During this reporting period, CIA identified approximately █ disseminations of Section 702-acquired data containing minimized United States person information. █ and as reported in prior joint assessments, CIA also permits some █

As noted above, due to

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

CIA initially cancelling all in-person visits in response to the coronavirus pandemic, NSD and ODNI were unable to review the referenced disseminations [REDACTED] to ensure compliance with CIA's minimization procedures during this reporting period. NSD and ODNI reviewed these [REDACTED] during a review that took place after the reporting period.

(U) CIA also tracks the number of files its personnel determine are appropriate for broader access and longer-term retention. CIA's minimization procedures must be applied to those files before they are retained or transferred to systems with broader access.<sup>43</sup> Figure 10 details the total number of files that were either retained or transferred, as well as the number of those retained or transferred files that contain identified United States person information. This current assessment reports the total number of files CIA transferred from December 2019 through May 2020. For reference, however, the number of files retained from prior assessment periods is also displayed in Figure 10. The percentage of retained or transferred files identified by CIA as potentially containing United States person information has remained consistently low.<sup>44</sup>

---

<sup>43</sup> ~~(S//NF)~~ [REDACTED]

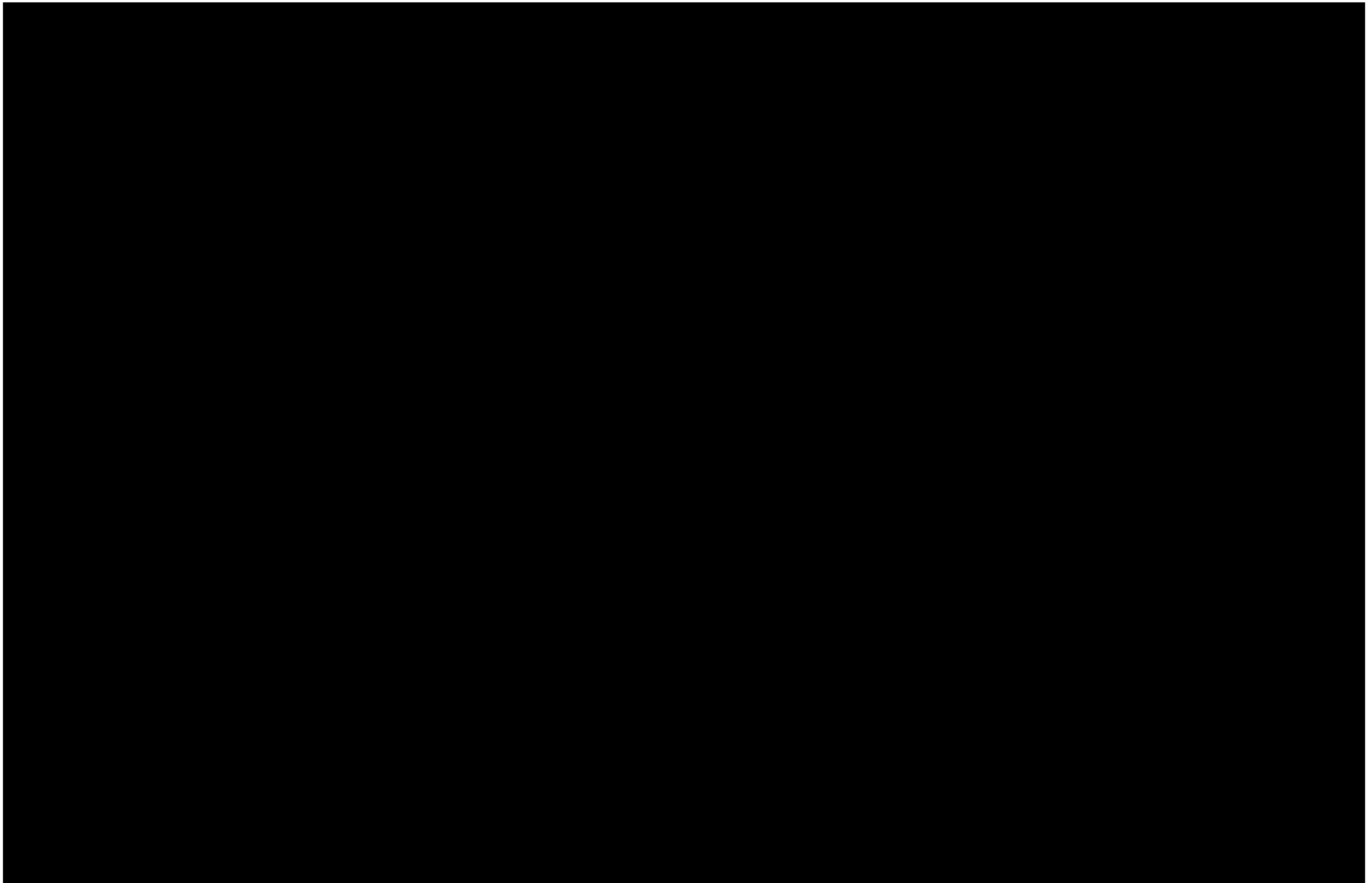
[REDACTED] In making those retention decisions, CIA personnel are required to identify any files potentially containing United States person information.

<sup>44</sup> ~~(S//NF)~~ For this reporting period, CIA analysts transferred a total of approximately [REDACTED] (2.7 percent) of which were identified by CIA as containing a communication with potential United States person information.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

**(U) Figure 10: Total CIA Files Retained or Transferred and Total CIA Files that Were Retained or Transferred which Contained Potential United States Person Information<sup>45</sup>**



(U) Figure 10 is classified ~~SECRET//NOFORN~~.

**(U) IV. Trends in NCTC Minimization**

(U) Beginning with the reporting period covering June 2017 through November 2017, the joint assessment now includes statistics regarding the total number of disseminations identified by NCTC as containing Section 702-acquired information. This number is classified and reported in Figure 11. Starting in November 2018, NCTC identified and provided to NSD and ODNI only disseminations containing minimized United States person information. Because NCTC only began obtaining unminimized Section 702-acquired data after the FISC approval of such in April 2017, there are only six six-month periods to report in this assessment.<sup>46</sup> This current joint assessment reports that the number of disseminations containing minimized United States person information, while low, increased from the previous reporting period.

<sup>45</sup> [REDACTED]

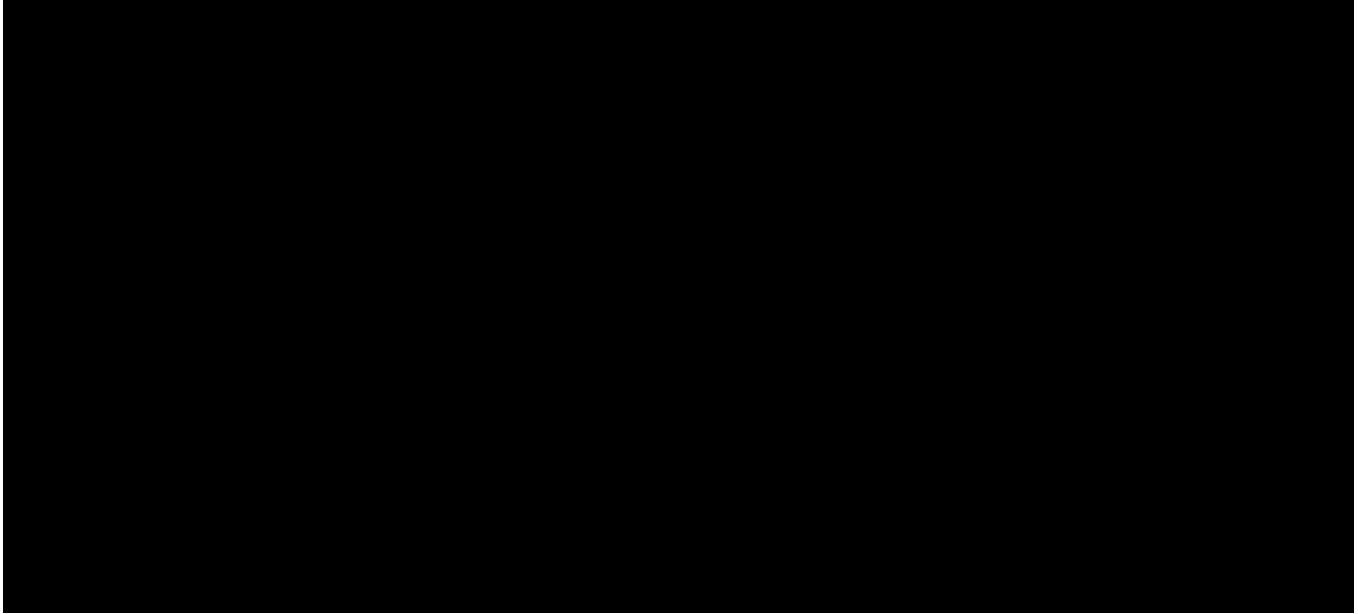
<sup>46</sup> ~~(S//NF)~~ The FISC's April 2017 opinion approved NCTC's 2016 minimization procedures allowing NCTC to obtain unminimized Section 702-acquired information. NCTC began receiving unminimized Section 702-acquired information on [REDACTED] May [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

**(U) Figure 11: Disseminations Identified by NCTC as Containing Minimized Section 702-Acquired Information**



(U) Figure 11 is classified ~~SECRET//NOFORN~~.

~~(S//NF)~~ During this reporting period, NCTC identified and provided to NSD and ODNI approximately [REDACTED] disseminations of Section 702-acquired data containing minimized United States person information. This represented a 47.5 percent increase in disseminations containing minimized United States person information when compared to the previous reporting period.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~**(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS**

(U) The joint oversight team finds that during this reporting period, the agencies have continued to implement their procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the Section 702 authorities are appropriately directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes have been put in place to implement these authorities and to impose internal controls for compliance and verification purposes.

(U) However, notwithstanding a focused and concerted effort by FBI personnel to comply with the requirements of Section 702, misunderstandings regarding FBI's systems and FBI's querying requirements continued to cause a large number of query errors. While the number of FBI compliance incidents decreased substantially compared to the previous reporting period, this assessment still reports a large number of FBI compliance incidents related to querying, and, in particular, FBI's use of "batch queries."<sup>47</sup> Although reported to the FISC during this reporting period, some of these query incidents occurred prior to certain remedial steps taken by the FBI in late 2019. In addition, these query incidents occurred prior to the FBI's implementation in 2021 of significant corrective measures to prevent the query compliance issues. These corrective measures are addressed further below.

(U) FBI amended its querying procedures in 2019 in response to concerns raised by the FISC and the FISC-R regarding the sufficiency of those procedures with respect to FBI's queries. The FISC ultimately determined that FBI's amended querying procedures were adequate, and the joint oversight team engaged with FBI to implement those amended procedures and provided the FISC with periodic reporting regarding that implementation, including with respect to systemic changes and additional training of FBI personnel.<sup>48</sup> These incidents and remedial measures are detailed below and will be updated in future assessments, as appropriate.

---

<sup>47</sup> ~~(S//NF)~~ The number of FBI minimization and querying errors for the current reporting period was [REDACTED] compared to the [REDACTED] minimization and querying errors in the previous reporting period.

<sup>48</sup> (U) On 08 October 2019, the ODNI posted, on *IC on the Record*, documents related to the 2018 certifications, including the FISC's October 2018 opinion, the FISC-R's July 2019 opinion, the FISC's September 2019 opinion, and FBI's amended querying procedures, dated August 2019. Specifically, in its October 2018 opinion, the FISC found that certain parts of FBI's procedures concerning the querying of United States persons were not sufficient. The Government appealed this decision to the FISC-R, which affirmed the FISC's decision in part. The Government subsequently submitted amended FBI querying procedures to address the issues raised by the FISC and the FISC-R, and the FISC found that the amended procedures were sufficient.

(U) Subsequently, while outside this reporting period, the FISC revisited FBI's non-compliant queries in its December 2019 opinion authorizing the 2019 Section 702 certifications, and its November 2020 opinion authorizing the 2020 Section 702 certifications; these opinions and other documents related to the 2019 and 2020 Section 702 certifications were released on 04 September 2020 and 26 April 2021, respectively, on *IC on the Record*. As it pertained to FBI's querying procedures, the FISC's opinion regarding the 2019 Section 702 certifications found that FBI was following its schedule for implementing the training and system modifications necessary to comply with its querying procedures. The FISC's opinion regarding the 2020 Section 702 certifications found that FBI's querying

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(U) As noted in prior joint assessments, in the cooperative environment the implementing agencies have established, an action by one agency can result in an incident of noncompliance with another agency's procedures. For example, an "NSA compliance incident" could be caused by typographical errors contained in another agency's nomination to NSA for tasking.

(U) Each compliance incident for this current reporting period is described in detail in the corresponding Section 707 Report. This joint assessment does not reiterate the compliance incidents set forth in the Section 707 Report. It does, however, examine those incidents to assess broader implications and to determine whether the agency's corrective measures address those implications.

(U) Even a small number of incidents can have the potential of carrying broader implications, and a small number of actions can result in numerous incidents also having broad implications, as is the case for FBI "batch" querying incidents. Thus, the joint assessment provides NSD and ODNI's analysis of compliance incidents in an effort to identify existing patterns or trends that might identify underlying causes of those incidents. The joint oversight team then considers whether and how those underlying causes could be addressed through additional remedial or proactive measures and assesses whether the agency involved has implemented appropriate procedures to prevent recurrences. The joint oversight team continues to assist in the development of such measures, some of which are detailed below, especially as it pertains to investigating whether additional and/or new system automation may assist in preventing compliance incidents.

#### (U) **I. Compliance Incidents – General**

##### (U) **A. Statistical Data Relating To Compliance Incidents**

~~(S//NF)~~ As noted in the Section 707 Report, during this reporting period, there were a total of [REDACTED] compliance incidents that involved noncompliance with NSA's targeting, minimization, or querying procedures and [REDACTED] compliance incidents involving noncompliance with FBI's targeting, minimization, and querying procedures.<sup>49</sup> In addition, during this reporting period, there were [REDACTED] incidents of noncompliance with CIA's minimization and querying procedures and no incidents of noncompliance with NCTC's minimization and querying procedures. There were no identified instances of noncompliance by an electronic communication service provider issued a directive pursuant to Section 702(i) of FISA.

---

procedures were sufficient, but the Court expressed continued concern about FBI's practices involving United States person query terms.

<sup>49</sup> (U) As is discussed in the Section 707 report and below, some compliance incidents involve more than one element of the IC. Incidents have therefore been grouped not by the agency "at fault" but instead by the set of procedures such actions violated.

~~TOP SECRET//SI//ORCON//NOFORN~~

(U) Figure 12 puts those compliance incidents in the context of the average number of facilities subject to acquisition on any given day<sup>50</sup> during the reporting period.

**(U) Figure 12: Overall Compliance Incident Rate**

~~SECRET~~ [REDACTED]

(U) Total compliance incidents during reporting period (01 December 2019 – 31 May 2020)	
(U) Number of facilities on average subject to acquisition during the reporting period	
(U) Overall compliance incident rate: number of incidents divided by average number of facilities subject to acquisition	(U) 0.46 percent

(U) Figure 12 is classified ~~SECRET~~ [REDACTED]

(U) The 0.46 percent overall compliance incident rate represents a substantial decrease from the 20.28 percent overall compliance incident rate in the prior reporting period. While this is an improvement over prior reporting periods, as with the previous incident rate, the current reporting period’s overall compliance incident rate was predominantly impacted by FBI personnel misunderstanding the query standard in FBI’s querying procedures. These incidents – including the remedies – are discussed in detail below. As discussed above and detailed below, the manner in which this overall compliance incident rate is calculated results in an imperfect measure of the error rate for the Section 702 program during this reporting period. Additionally, as noted elsewhere, a significant portion of this reporting period occurred during the coronavirus pandemic, and the joint oversight team is not able to determine to what extent the decrease in the overall compliance incident rate reflects a decrease in the actual number of compliance incidents – whether as a result of the pandemic or improvements in compliance – as opposed to difficulties in discovering and reporting compliance incidents.

(U) As discussed below, notification delays are incidents in which the notification requirement contained in the targeting procedures was not satisfied. Substantive compliance incidents are not captured in this metric. If a compliance incident involved both a substantive error (for example, a tasking or detasking error) and the failure to meet the notification requirement, the substantive error was counted separately from the notification delay. For the majority of these notification delays, the only incident of non-compliance was the failure to comply with the

<sup>50</sup> [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

notification requirement. Accordingly, the joint oversight team determined that another valuable measure is to compare the overall compliance incident rate excluding notification delays. If the notification delay incidents are not included in the calculation, the overall compliance incident rate for this reporting period decreases slightly to 0.44 percent. The comparable incident rates in the previous two reporting periods were 20.24 percent and 6.9 percent, respectively.

(U) The joint oversight team assesses that the compliance incident rate – with and without the notification delay incidents – remained low and is a result of training, internal processes designed to identify and remediate potential compliance issues, and a continued focus by internal and external oversight personnel to ensure compliance with the applicable targeting, minimization, and querying procedures. As it pertains to FBI querying incidents, the joint oversight team identified a significant number of non-compliant queries, though far fewer than in prior reporting periods. The joint oversight team believes that the suspension of NSD’s FBI field office reviews in March 2020 was likely a significant factor in the decrease in identified incidents.<sup>51</sup> Notably, NSD conducted far fewer query audits than in past years. For example, in 2020, NSD conducted query audits of only six field offices, whereas NSD conducted query audits of 27 field offices in 2019 and 29 field offices in 2018. In addition, because certain FBI systems permit users to conduct multiple queries as part of a single batch job, a single action can result in thousands of improper queries; as such, the discovery of a single noncompliant batch job can substantially affect both the overall and FBI query compliance incident rates. Whether such a noncompliant batch job would or would not have been discovered in the temporarily suspended FBI field office reviews is unknown. As a result, the joint oversight team is unable to evaluate how FBI’s compliance with its querying procedures during this reporting period compares to other reporting periods. NSD and ODNI do assess, however, that query issues were a pervasive compliance challenge during the period of time covered by this joint assessment based on the results of NSD’s audits conducted during this and prior reporting periods, as well as the results of NSD’s remote audits in 2021, which reviewed historical queries conducted throughout 2020. The joint oversight team continues to work with FBI to reduce non-compliant queries and improve training and guidance regarding this issue.

(U) As explained in previous assessments, the joint oversight team periodically evaluates how and what data it collects to provide for more meaningful statistics. For example, the team considers whether there are other means of comparison – whether with the currently tracked actions or by implementing the tracking of certain other data – that could provide a better understanding of overall compliance. The joint assessment has traditionally compared the number of compliance incidents (*i.e.*, the “numerator”) to targeting activity during the reporting period, which is reflected as the average number of tasked facilities (*i.e.*, the “denominator”).

(U) While tracking this rate over consecutive years allows one to discern general trends as to how the Section 702 program is functioning overall from a compliance standpoint, it remains an imperfect proxy. A flaw with using this particular proxy is that certain types of incidents included in the numerator do not bear a relation to the targeting activity in the denominator. For example,

---

<sup>51</sup> (U) NSD generally conducts onsite reviews at FBI field offices. However, in response to the coronavirus pandemic, NSD temporarily suspended its onsite reviews in or about the middle of March 2020. NSD began conducting remote reviews in February 2021. Therefore, during this reporting period, NSD only conducted field office reviews between December 2019 and mid-March 2020.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

assessing a delayed detasking incident (which is an incident resulting from non-compliance with targeting procedures) as contained in the numerator to the average number of tasked facilities as contained in the denominator compares closely similar factors – both are directly related to tasking and must meet the requirements of the targeting procedures. However, the factors are not similar when comparing an improper dissemination incident or an improper query (which are incidents resulting from non-compliance with minimization and querying procedures) to the average number of tasked facilities. Minimization and querying incidents implicate the requirements of the minimization and querying procedures, whereas the tasking of a facility implicates the requirements of the targeting procedures. In addition, the number of query and dissemination incidents that can occur in a reporting period are largely independent from the number of facilities tasked during a period, as queries and disseminations can involve facilities that are no longer tasked – or were never tasked – pursuant to Section 702, and multiple queries or disseminations can be made in relation to a single facility. Conceivably, minimization incidents should be compared to the number of total minimization actions, but we are currently unable to count or track minimization actions in that manner. Adding to the dissimilarity is that multiple agencies' (NSA, FBI, CIA, and NCTC) incidents – as well as incidents by service providers – are counted in the overall compliance incident rate, but only two agencies (NSA and FBI) actually conduct targeting activity pursuant to their respective targeting procedures, and only NSA's targeting activities are included in the denominator.

(U) As with prior reporting periods, the number of compliance incidents in the numerator that do not bear a relation to the denominator (in particular, FBI query errors) outweighs the number of compliance incidents that do bear a relation to the denominator (*e.g.*, NSA targeting errors). Accordingly, readers should understand that the 0.46 percent overall compliance incident rate is an imperfect representation of the error rate for the Section 702 program during this reporting period.

(U) This assessment also provides an additional metric: the NSA targeting compliance incident rate (see Figures 15 and 16). Additionally, the joint oversight team has decided that, because FBI query errors comprised a substantial number of the incidents reported during this reporting period, this assessment includes – and, depending on the type of errors that were reported during the applicable period, potentially future assessments will include – a query error rate for FBI (see Figure 18).

(U) Separating the targeting errors from the minimization and query errors allows for another layer of evaluation. We provide these additional metrics to advance the understanding of the incidents' impact and the causes of those incidents. These metrics are provided after an explanation of the categories of compliance incidents so that the new metrics can better be understood.

(U) Notwithstanding the issues discussed above, the current assessment provides the overall compliance incident rates in Figures 12 and 13 so that readers can see the size of the movements as compared to historical periods in order to place the number of FBI query errors reported during this

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

reporting period in the context of a rate that has been used historically, as these query errors were the driving factor in the rate movements over the last few reporting periods.<sup>52</sup>

### (U) **B. NSA's Compliance Incidents: Categories and Number of Incidents**

(U) As it has been historically, most of the compliance incidents occurring during this reporting period – excluding FBI querying incidents – involved non-compliance with NSA's targeting, minimization, or querying procedures. This largely reflects the centrality of NSA's targeting, minimization, and querying efforts in the Government's implementation of the Section 702 authority. The compliance incidents involving NSA's targeting, minimization, or querying procedures have generally fallen into the categories below. However, in some instances, an incident may involve more than one category of noncompliance.

#### (U) Incidents of non-compliance with NSA's Targeting Procedures:

- (U) *Tasking Issues*. This category involves incidents where noncompliance with the targeting procedures resulted in an error in the initial tasking of the facility.
- (U) *Detasking Issues*. This category involves incidents in which the facility was properly tasked in accordance with the targeting procedures, but errors in the detasking of the facility caused noncompliance with the targeting procedures.
- (U) *Overcollection*. This category involves incidents in which NSA's collection systems, in the process of attempting to acquire the communications of properly tasked facilities, also acquired data regarding untasked facilities, resulting in "overcollection."
- (U) *Notification Delays*. This category involves incidents in which a notification requirement contained in the targeting procedures was not satisfied.<sup>53</sup>
- (U) *Documentation Issues*. This category involves incidents where the determination to target a facility was not properly documented as required by the targeting procedures.

#### (U) Incidents of non-compliance with NSA's Minimization and Querying Procedures:

- (U) *Minimization and Querying Issues*. This category involves incidents relating to NSA's non-compliance with its minimization and querying procedures.

(U) *Other Issues*. This category involves incidents that do not fall into one of the six above categories. In these instances, the joint oversight team will assess each incident to determine if it resulted from non-compliance with NSA's targeting, minimization, or querying procedures and account for those incidents accordingly.

---

<sup>52</sup> (U) Note that because of the imperfections described above, and because FBI query errors are only one factor in the overall compliance incident rate, a period-on-period comparison of the rate will still not provide an entirely accurate measure of the increase in FBI query errors.

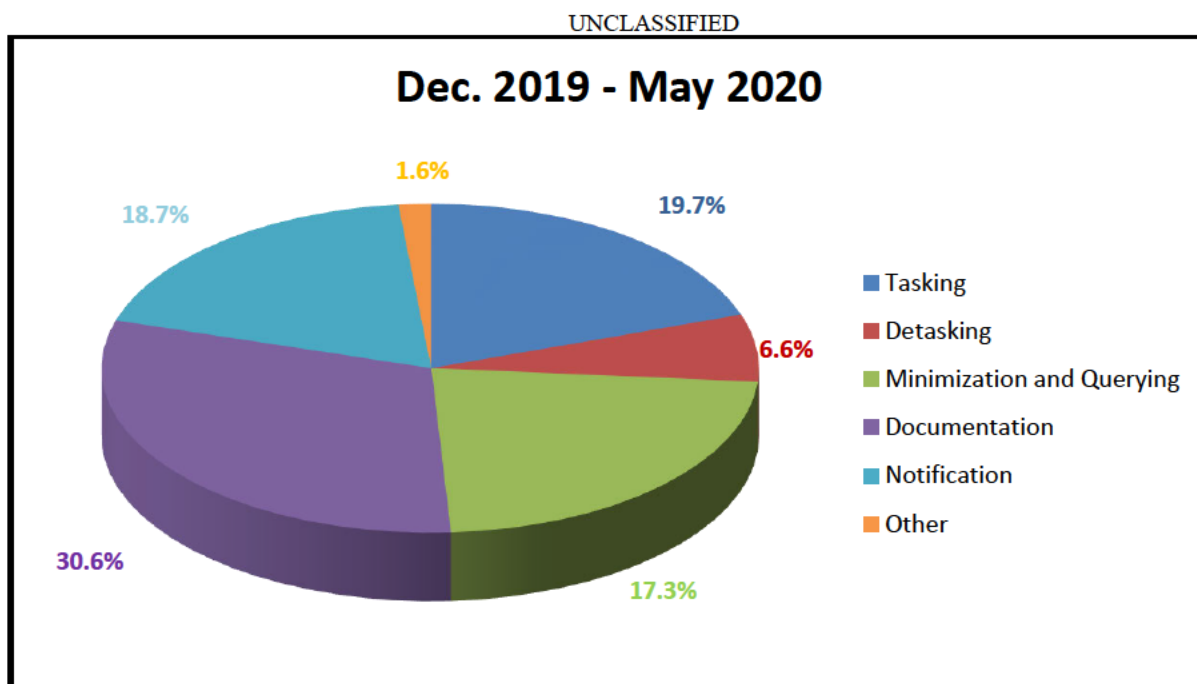
<sup>53</sup> (U) A compliance incident may involve both a failure to meet the notification requirement and a substantive error (for example, a tasking or detasking error). However, in those instances, the substantive error was counted separate from the notification delay. For the majority of delayed notification incidents, the only incident of non-compliance was the failure to comply with the notification requirement.

~~TOP SECRET//SI//ORCON//NOFORN~~

(U) While the above categories specifically pertain to NSA incidents, FBI’s targeting incidents categories and all other agencies’ minimization and querying incidents categories generally align to those NSA categories. Because only NSA and FBI are permitted to target pursuant to Section 702, only NSA and FBI have targeting procedures (which have been publicly released). All four agencies have minimization and querying procedures (which have been publicly released). Compliance incidents by FBI, CIA, and NCTC are discussed in their respective sections below.

(U) These categories are helpful for purposes of reporting and understanding the compliance incidents. Because the actual number of incidents remains classified, Figure 13A depicts the percentage of NSA compliance incidents in each category that occurred during this reporting period, whereas Figure 13B provides that actual classified number of NSA incidents.

**(U) Figure 13A: Percentage Breakdown of Compliance Incidents Involving NSA’s Targeting, Minimization, and Querying Procedures**



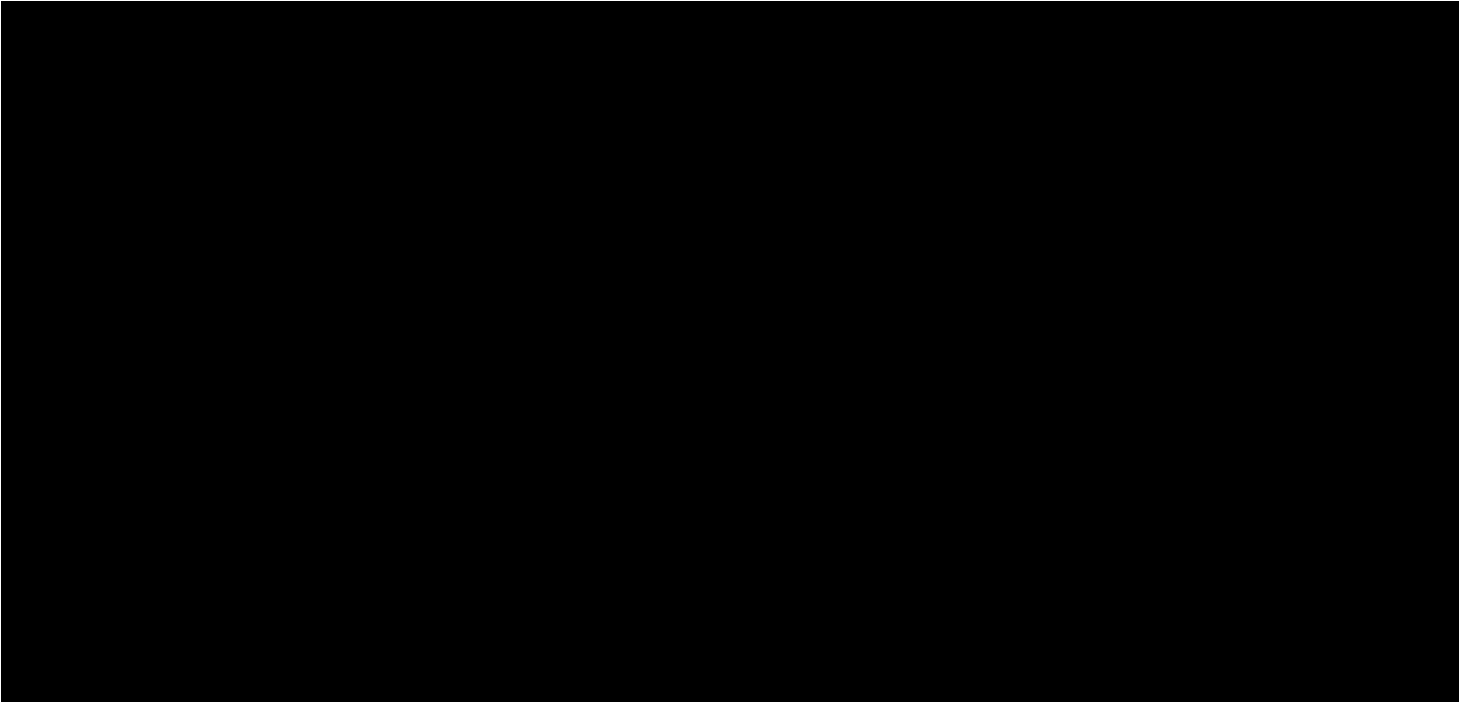
(U) Figure 13A is UNCLASSIFIED

While accurately depicted on the pie chart, the minimization and querying percentage in Figure 13A was mislabeled. It should read 22.7% rather than 17.3%.



~~TOP SECRET//SI//ORCON//NOFORN~~

**(U) Figure 13B: Number of Compliance Incidents Involving NSA’s Targeting, Minimization, and Querying Procedures**



(U) Figure 13B is classified ~~SECRET//NOFORN~~

(U) As Figures 13A and 13B demonstrate, during this reporting period, documentation errors accounted for the largest portion of incidents across all categories. Minimization and querying incidents and tasking errors accounted for the second and third largest percentage of incidents, respectively, followed by notification delays. Tracking the proportion of incidents allows for the joint oversight team to identify trends and to address the non-compliance with appropriate remedies. Being able to do so is important for a variety reasons, especially as it pertains to more substantive tasking and detasking compliance incidents that can (but do not always) involve collection involving a facility used by a United States person or an individual located in the United States. Furthermore, the joint oversight team also focuses on incidents of noncompliance with minimization and querying procedures because these types of incidents may involve information concerning United States persons.

~~(S//NF)~~ More specifically, the number of tasking incidents decreased from [REDACTED]; detasking incidents decreased from [REDACTED]; minimization and querying incidents decreased from [REDACTED]; documentation incidents increased from [REDACTED]; and “other” category incidents decreased from [REDACTED]. The number of notification delays decreased from [REDACTED]. There were zero overcollection incidents in this period.

(U) As mentioned above, separating the targeting errors from the minimization and querying errors allows for another layer of evaluation as opposed to comparing all of the errors together. By narrowing the focus on errors implicating NSA’s targeting procedures, Figure 14 provides the NSA targeting compliance incident rate for this current reporting period. This metric compares similar

~~TOP SECRET//SI//ORCON//NOFORN~~

factors: NSA’s number of “targeting incidents” (*i.e.*, the “numerator”) to NSA’s targeting activity of the number of average tasked facilities (*i.e.*, the “denominator”). The number of NSA’s “targeting incidents” includes the following categories of incidents that implicate NSA’s targeting procedures: tasking errors, detasking delays, documentation errors, notification delays, and overcollection incidents. As explained above, incidents that fall under the “other issues” category may be included as well if those constituted errors in following NSA’s targeting procedures.

**(U) Figure 14: NSA Targeting Compliance Incident Rate**

~~SECRET~~ [REDACTED]

[REDACTED]	
(U) NSA compliance incidents relating to NSA’s targeting procedures, during reporting period (01 December 2019 – 31 May 2020)	[REDACTED]
(U) Number of facilities on average subject to acquisition during the reporting period	[REDACTED]
(U) NSA targeting compliance incident rate: number of targeting incidents divided by average number of facilities tasked to acquisition	(U) 0.10 percent

(U) Figure 14 is classified ~~SECRET~~ [REDACTED]

(U) This NSA targeting compliance incident rate percentage, in and of itself, does not provide a full measure of compliance in the program. A single incident, for example, may involve multiple facilities. Also, a single action may result in numerous incidents. Furthermore, other incidents, such as notification delays (described further below) may occur with frequency, but have limited significance with respect to United States persons.

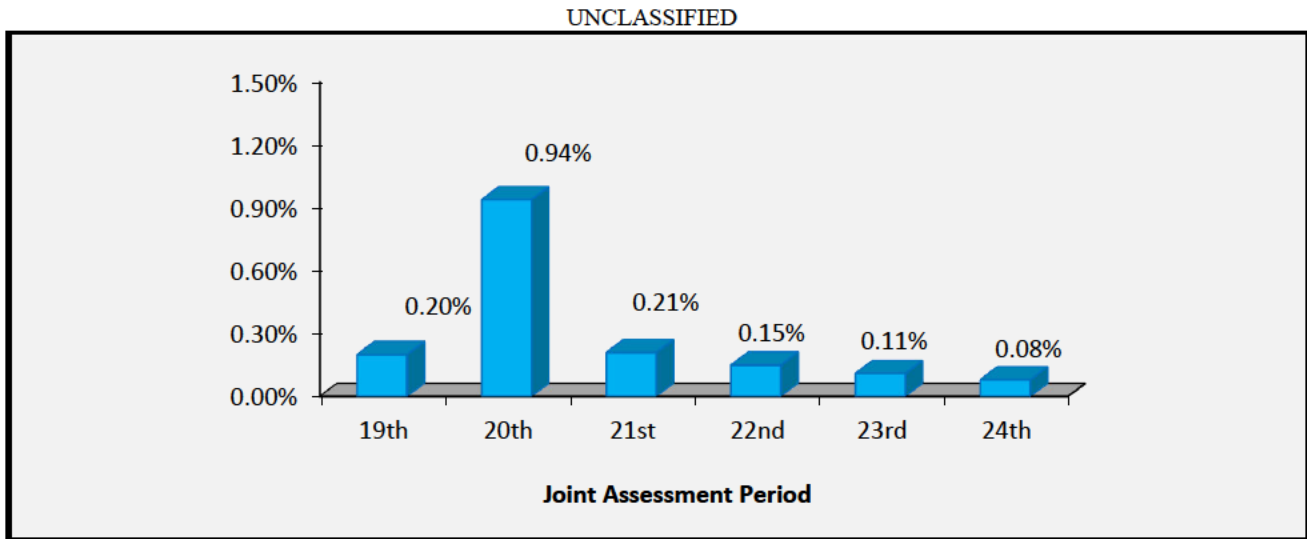
(U) The joint oversight team has determined that excluding NSA’s notification delays incidents from NSA’s targeting compliance incident rate provides another measure of compliance.<sup>54</sup> Thus, Figure 15 shows an adjusted NSA targeting compliance incident rate of 0.08 percent, not including notification delay errors (as compared to 0.10 percent of NSA targeting compliance incident rate, including notification errors).<sup>55</sup> As Figure 15 shows, NSA’s targeting compliance incident rate (not including notification delays) during this reporting period was at its lowest level since the inclusion of this statistic.

<sup>54</sup> (U) Notification delays are violations of the notification requirement contained in the targeting procedures. Substantive compliance incidents are not captured in this metric. If a compliance incident involved both a substantive error (for example, a tasking or detasking error) and the failure to meet the notification requirement, the substantive error was counted separately from the notification delay. For the majority of the notification delays, the only incident of non-compliance was the failure to comply with the notification requirement.

<sup>55</sup> (U) As described in prior joint assessments, the increase from 0.20 percent in the 19<sup>th</sup> reporting period to 0.94 percent in the 20<sup>th</sup> reporting period was primarily a result of one NSA office’s misunderstanding regarding how a targeting tool functioned, which resulted in an abnormally large number of targeting incidents.

~~TOP SECRET//SI//ORCON/NOFORN~~

(U) **Figure 15: NSA Targeting Compliance Incident Rate (as the number of incidents divided by the average number of facilities tasked), *not* Including Notification Delays**

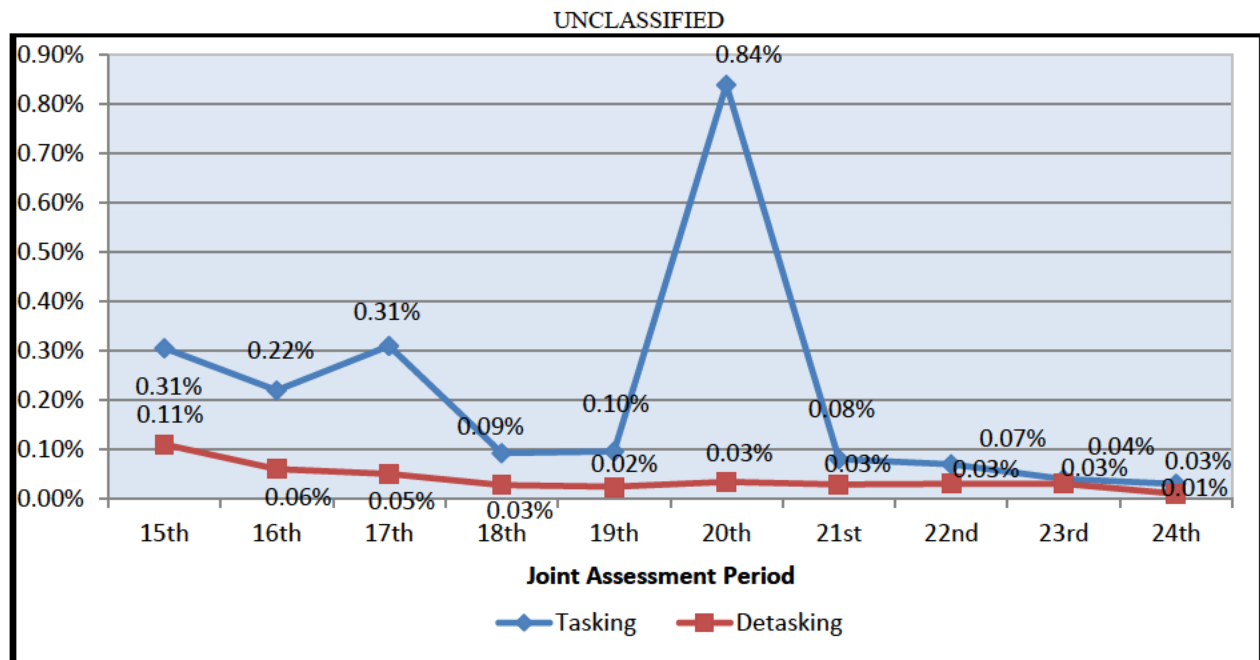


(U) Figure 15 is UNCLASSIFIED.

(U) Whereas Figure 15 depicts NSA targeting incidents by combining all targeting incidents, except for notification delays, Figure 16 depicts NSA's compliance incident rates individually for tasking and detasking incidents. Figure 16 separates those types of incidents for more granularity and understanding of the trends for each. As previously calculated and reported, the tasking and detasking incident rate is compared to the average number of facilities on collection for the given reporting period. While these tasking and detasking incidents are grouped in a single chart for a comparison, the tasking and detasking incidents are not relational to each other (*i.e.*, an increase or decrease in the rate of tasking incidents does not result in an increase or decrease in the detasking incident rate).

~~TOP SECRET//SI//ORCON/NOFORN~~

(U) **Figure 16: Tasking and Detasking Incident Compliance Rates**



(U) Figure 16 is UNCLASSIFIED.

(U) It is important to note that, while Figure 16 provides a visual into trends of non-compliance, the non-compliance rate is less than 1 percent. The tasking and detasking incident compliance rate has varied by fractions of a percentage point as compared to the average size of the collection.<sup>56</sup> The tasking incident rate decreased to 0.03 percent during this reporting period, which comports with its historically low rate.<sup>57</sup> The tasking compliance incident rate involving facilities used by United States persons remained almost zero. Detasking errors more often involve delays in detasking a facility that the Government learns is used by a United States person or an individual located in the United States, who may or may not have been the targeted user. The percentage of compliance incidents involving detasking incidents has remained consistently low. The detasking compliance incident rate involving facilities used by United States persons was also close to zero.

<sup>56</sup> (U) Tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have reasonably known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United States persons or persons located in the United States. Detasking errors more often involve delays in detasking a facility that the Government learns is used by a United States person or an individual located in the United States, who may or may not have been the targeted user. In addition, a single detasking delay may involve multiple facilities that were not timely detasked.

<sup>57</sup> (U) As previously noted, the increase in the tasking incident rate reported in the 20<sup>th</sup> Joint Assessment was primarily due to a single NSA targeting office misunderstanding how to use a targeting tool.

~~TOP SECRET//SI//ORCON//NOFORN~~**(U) C. FBI: Number of Compliance Incidents**

(U) The total number of compliance incidents identified relating to FBI's targeting procedures substantially decreased as compared to the last period. The number of errors relating to FBI's minimization and querying procedures also significantly decreased this reporting period. The joint oversight team believes that the temporary suspension of NSD's FBI field office reviews starting in mid-March 2020, due to the coronavirus pandemic, and the potentially related non-identification of extremely large batch query errors were significant factors in this decrease. In recent years, FBI field office reviews have been responsible for discovering a significant portion of FBI's minimization and querying incidents that are reported in each joint assessment. Because FBI field office reviews were suspended during a portion of this reporting period, incidents that would typically be discovered by NSD during those field office reviews would not have been discovered while the reviews were suspended.<sup>58</sup>

(U) Figure 17 shows the classified number of incidents for the last 10 reporting periods. The joint oversight team assesses that the increase in identified FBI errors beginning in the 19<sup>th</sup> reporting period is attributable to various factors. In particular, NSD increased its focus on reviewing FBI querying practices; this focus resulted in NSD's increased experience in evaluating those types of FBI queries and NSD's increased knowledge of FBI systems storing Section 702-acquired information. The joint oversight team believes that this increased focus and experience, along with other factors, resulted in NSD identifying a larger number of non-compliant queries.

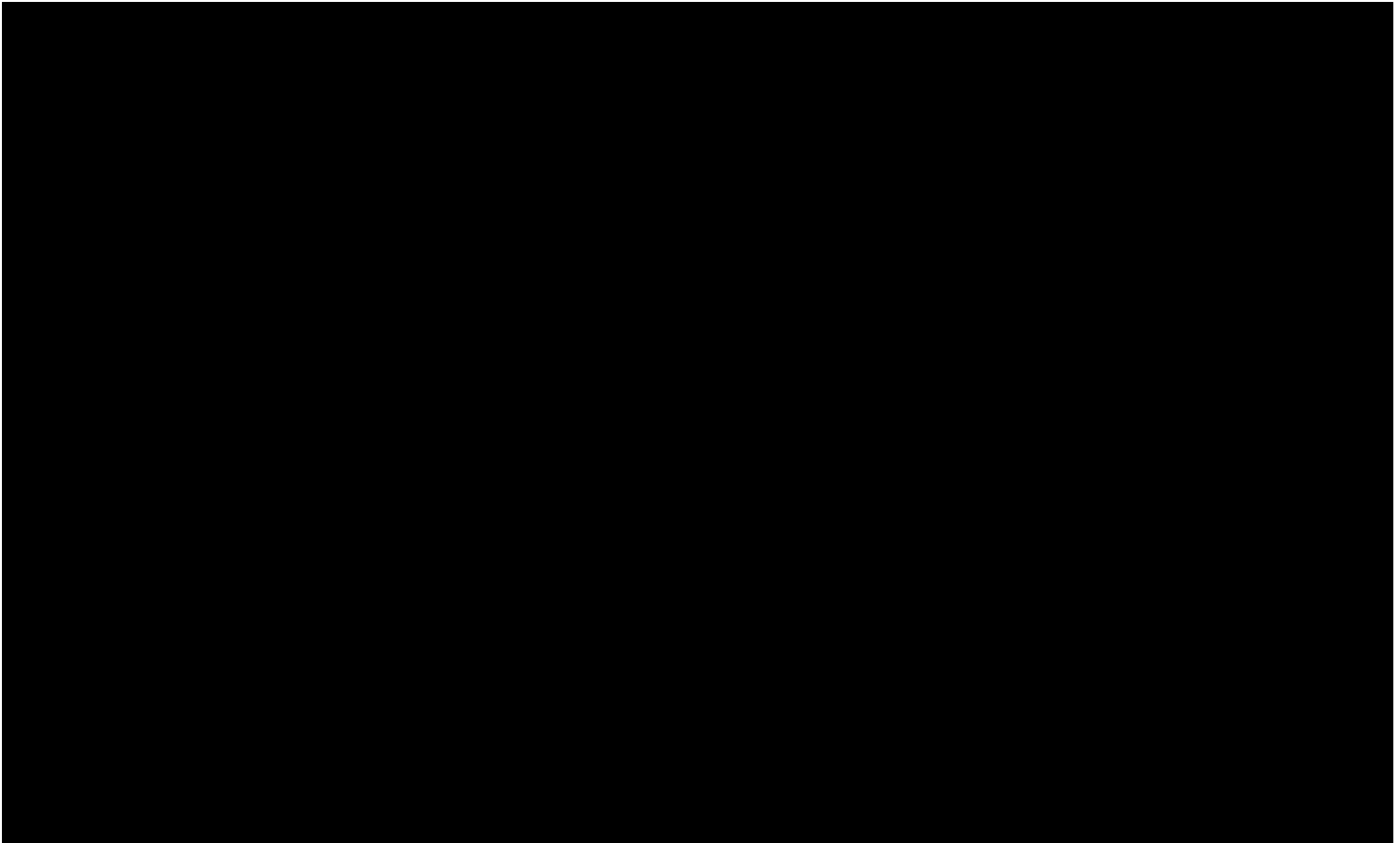
---

<sup>58</sup> ~~(S//NF)~~ During this reporting period, [REDACTED] incidents of non-compliance with FBI's targeting, minimization, or querying procedures were identified. Most of these incidents pertain to non-compliant queries, and in particular, one compliance error comprised [REDACTED] or about 37 percent, of the [REDACTED] incidents. The FBI system in which the non-compliant batch queries were conducted was FBI [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

**(U) Figure 17: Number of Compliance Incidents Involving FBI's Targeting, Minimization, and Querying Procedures**



(U) Figure 17 is classified ~~SECRET//NOFORN~~.

(U) In light of the joint oversight team's decision to provide the NSA targeting compliance incident rate above, the joint oversight team determined that it would also increase transparency to include a metric representing the FBI targeting compliance incident rate. During this reporting period, the FBI targeting compliance incident rate was 0.007 percent, a slight increase from the previous period (0.005 percent).<sup>59</sup> Historically, this rate has remained well-below one percent. The joint oversight team assesses that FBI's compliance with respect to targeting is a result of its training, systems, and processes.

(U) As discussed above, the joint oversight team has decided to provide a metric depicting FBI's query error rate. Figure 18 provides the FBI query compliance incident rate, which is

---

<sup>59</sup> ~~(S//NF)~~ The FBI targeting compliance incident rate is calculated as the total number of FBI targeting errors reported during the reporting period, expressed as a percentage of the total number of facilities for which FBI approved a request [REDACTED] during the reporting period. As noted above, the joint oversight team does not review all such approved requests. The joint oversight team only reviews checklists and supporting documentation relating to approved requests for which information was returned by FBI's database queries. In addition, during this reporting period, the joint oversight team only reviewed checklists and supporting documentation for a sample of such approved requests.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

calculated as the total number of FBI query compliance incidents reported by NSD to the FISC during the reporting period, expressed as a percentage of the total number of FBI queries audited by NSD in connection with the field office reviews during which NSD identified the FBI query compliance incidents reported to the FISC during the reporting period. As noted above, due to the pandemic, NSD had suspended its query reviews during a significant portion of this reporting period, and only conducted such reviews between December 2019 and early-March 2020.

**(U) Figure 18: FBI Query Compliance Incident Rate**

~~SECRET//NOFORN~~

(U) FBI query compliance incidents reported to the FISC during the reporting period (01 December 2019 – 31 May 2020)	
(U) Number of FBI queries audited by NSD in connection with field office reviews during which NSD identified the FBI query compliance incidents reported to the FISC during the reporting period <sup>60</sup>	
(U) FBI query compliance incident rate: number of query incidents reported, divided by number of queries audited	(U) 0.82 percent

(U) Figure 18 is classified ~~SECRET//NOFORN~~.

(U) The FBI compliance incident rate of 0.82 percent is a significant decrease from the 36.59 percent incident rate reported in the prior reporting period. While the total number of queries audited by NSD decreased by 21.63 percent, a decrease attributable to the temporary suspension of reviews due to the pandemic, the FBI query compliance incident rate decreased by 98.22 percent. The joint oversight team assesses that the difference between these two decreases is likely attributable to the fact that a certain FBI system permits users to conduct multiple queries as part of a single batch job, such that a single action can result in thousands of improper queries; therefore, the discovery of a single noncompliant batch query can substantially affect both the overall and FBI compliance incident rates. While, as discussed below, a batch query error was found in this reporting period, no identified batch query incidents in this reporting period involved thousands of queries, as was the case in the prior reporting periods. Even without large scale batch queries during this period, NSD identified query compliance issues in each field office audited during this reporting period and during calendar year 2019.<sup>61</sup> And, since NSD resumed its query audits in 2021, NSD has continued to identify query compliance incidents during each field office remote audit. FBI implemented certain remedial measures in fall 2019 to address query compliance issues and, since that time, the joint oversight team has continued to work with FBI to take additional

<sup>60</sup> (U) This number also includes the number of FBI queries audited by NSD in connection with any field office reviews completed by NSD during this reporting period for which no FBI query compliance incidents were discovered.

<sup>61</sup> (U) In 2018, NSD identified query compliance incidents in 26 of 29 field offices audited. In 2019, query errors were identified in all 27 field offices audited, and in 2020, query errors were identified in all six offices audited.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

corrective actions to address the query compliance issues. The remedial measures undertaken by FBI are discussed further below.

(U) In connection with its reviews at FBI field offices, NSD reviews a sample of queries conducted by FBI personnel in FBI systems that contain unminimized FISA-acquired information, including Section 702-acquired information. FBI provides NSD with logs of all the queries conducted in its systems during a given three-month period preceding the relevant field office review. NSD reviews the query logs and then consults with FBI personnel to obtain additional facts regarding the queries that were conducted. It is possible that some of the queries in the logs provided by FBI were not run against Section 702-acquired data, as NSD's query audits are designed to review compliance with FBI's query requirements in all of its applicable FISA procedures.<sup>62</sup> The FBI query error rate may also include identical queries that were conducted multiple times. For example, if NSD discovered that the same improper query was conducted on two separate occasions, those would be counted as two compliance incidents.

(U) In addition, as described below in Section III, certain of the query errors reported during this reporting period were discovered through National Security Reviews (NSRs) conducted by NSD, rather than through minimization or query reviews. As part of these NSRs, NSD reviews a sample of FBI predicated investigations and assessments opened under the FBI Attorney General Guidelines for Domestic Operations and determines whether there is sufficient predication to support the investigations and whether the assessments had authorized purposes. For example, NSD may identify that FBI conducted queries for an assessment that lacked an authorized purpose. Because that assessment lacked an authorized purpose, it can no longer be said that the query conducted in furtherance of that assessment is reasonably likely to retrieve foreign intelligence information or evidence of a crime. For instance, if NSD discovers that an assessment lacked an authorized purpose because it was solely based on First Amendment-protected activity, then any query made in furtherance of that assessment will not satisfy the querying standard. If NSD discovers improper queries during an NSR, NSD will ask FBI to provide logs of all the queries conducted in connection with the relevant national security assessment. The number of such improper queries is included in the numerator of the FBI query compliance incident rate, and the total number of queries documented in the query logs conducted against FISA-acquired information in relation to the assessment is included in the denominator.

(U) Neither the number of incidents reported in Figure 17, nor the FBI query compliance incident rate in Figure 18, is based on the number of compliance incidents that *occurred* during a given reporting period. Rather, each is based on the number of incidents that were *reported* to the FISC as compliance incidents during the reporting period. There may be delays in resolving and reporting compliance incidents after they are first identified, in part, because of delays in the Government's investigation while FBI gathers the relevant facts, or while FBI and NSD discuss whether the facts of a matter constitute a compliance incident. Incidents that occur during a given reporting period may, accordingly, be reported over multiple assessments, and the number of

---

<sup>62</sup> (U) FBI personnel may elect to run queries against FISA Titles I, III, and V but not against Section 702-acquired information. The query logs reviewed by NSD for its query audits include queries of information acquired pursuant to all FISA authorities, and the joint assessment team has not attempted to identify and exclude any queries that were included in the query logs but not run against Section 702-acquired information.

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

incidents reported in a given assessment may include incidents that occurred during multiple periods. The number of query compliance incidents reported in Figure 17, and the FBI query compliance incident rate in Figure 18, may, therefore, include queries audited by NSD during the reporting period for a prior joint assessment.

(U) In addition, because of the delays in resolving and reporting certain compliance incidents, incidents discovered at a single field office review may be reported during different reporting periods. When that occurs, the total number of FBI queries audited by NSD in connection with the relevant field office review is included in the denominator of the FBI query compliance incident rate for both reporting periods, even though the total number of FBI query compliance incidents discovered as a result of auditing those queries is split between reporting periods. There were two field office reviews for which some, but not all, of the FBI query compliance incidents were reported during this reporting period.

(U) Although each of the metrics in Figure 17 and Figure 18 has limitations, the joint oversight team believes that they nevertheless provide informative measures of FBI's compliance with its querying procedures.

**(U) D. CIA and NCTC: Number of Compliance Incidents**

~~(S//NF)~~ There were [REDACTED] incidents during this reporting period that involved CIA's minimization and querying procedures,<sup>63</sup> an increase from the [REDACTED] incidents reported in the previous reporting period. The joint oversight team assesses, however, that this is not a reflection on CIA compliance overall. CIA still maintains a strong compliance record as a result of training, systems, and processes that were implemented when and have been in place since the Section 702 program was developed to ensure compliance with its minimization and querying procedures and the work of its internal oversight team.

~~(S//NF)~~ There were no incidents during this reporting period that involved NCTC's minimization and querying procedures, which is a decrease from the [REDACTED] incidents during the previous reporting period.<sup>64</sup> The joint oversight team assesses that NCTC's overall compliance is a result of its training, systems, and process that were implemented when NCTC was authorized to receive certain unminimized Section 702-acquired information.

(U) Figure 19 provides the classified number of minimization and querying errors that involved CIA for the last 10 reporting periods and NCTC for reporting periods beginning with the 19<sup>th</sup> assessment period.

---

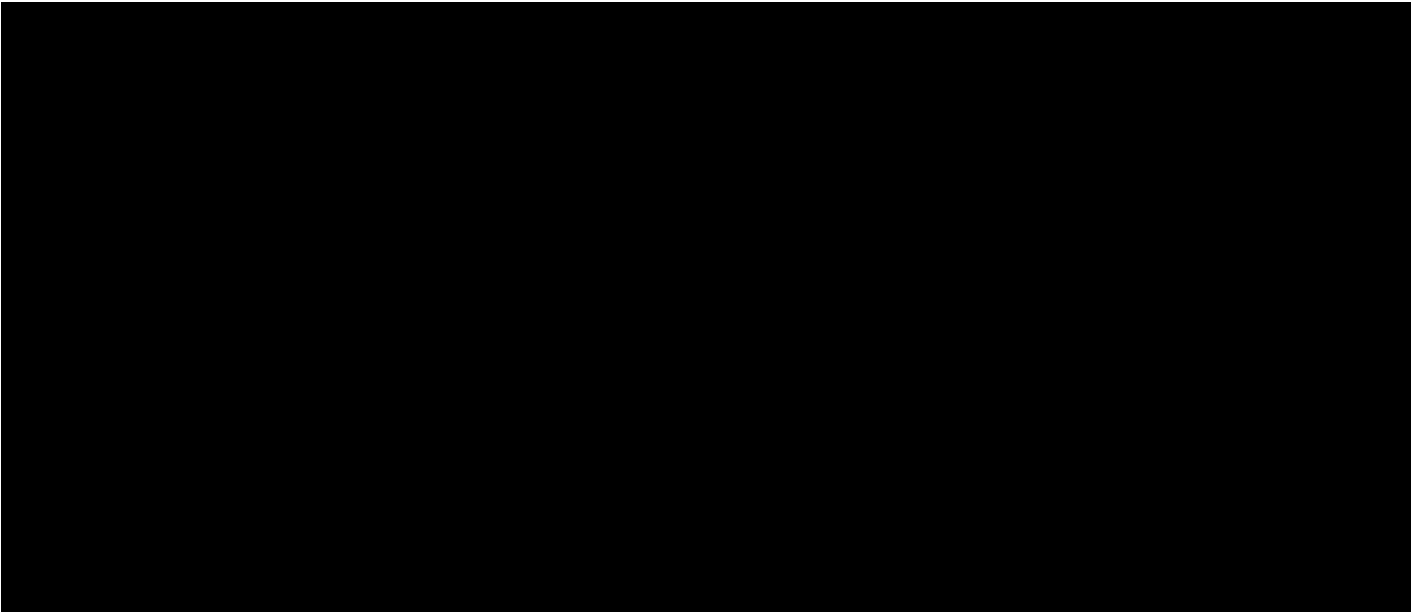
<sup>63</sup> (U) Recall that CIA does not have targeting procedures and may not target. Because CIA only has minimization and querying procedures, errors can only occur as it pertains to its minimization and querying procedures.

<sup>64</sup> (U) Recall that NCTC does not have targeting procedures and may not target. Because NCTC only has minimization and querying procedures, errors can only occur as it pertains to its minimization and querying procedures.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

**(U) Figure 19: Number of Compliance Incidents Involving CIA's or NCTC's Minimization and Querying Procedures**



(U) Figure 19 is classified ~~SECRET//NOFORN~~.

**(U) E. Service Providers: Number of Compliance Incidents**

(U) Finally, there were no incidents of non-compliance caused by errors made by communications service providers in this reporting period, which represents a decrease from the single incident reported in the prior reporting period. The joint oversight team assesses that the historically low number of errors by the communications service providers is the result of continuous efforts by the Government and providers to ensure that lawful intercept systems effectively comply with the law while protecting the privacy of the providers' customers.

**(U) II. Review of Compliance Incidents – NSA Targeting, Minimization, and Querying Procedures**

(U) As with the prior joint assessment, this joint assessment takes a broad approach and discusses the trends, patterns, and underlying causes of the compliance incidents reported in the Section 707 Report. The Section 707 Report provides further details regarding each individual incident and information on applicable remedial and mitigating actions. For each individual incident in the Section 707 Report, details are provided as to how any erroneously acquired, disseminated, or queried information was handled through various purge, recall, and deletion processes. Information is also provided about personnel remediation and, when applicable, wider training efforts to address incidents. In certain instances, processes or technical tools are adjusted, as appropriate, to remedy the incidents, to mitigate impact, and to reduce the potential for future incidents.

(U) The joint oversight team believes that analyzing the trends of those incidents, especially in regard to their causes, helps the agencies focus resources, avoid future incidents, and improve

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

overall compliance. The joint assessment primarily focuses on incidents involving NSA's targeting, minimization, and querying procedures, the volume and nature of which are better-suited to detecting such patterns and trends. The following subsections examine incidents of non-compliance involving NSA's targeting, minimization, and querying procedures.

(U) The NSA compliance incident rate for this reporting period (calculated as the total number of compliance incidents involving NSA's Section 702 procedures, *divided by* the average number of tasked facilities) is 0.13 percent and represents a decrease from the NSA compliance incident rate of 0.20 percent in the previous reporting period.

(U) Most of those incidents did not involve United States persons, and instead involved matters such as typographical or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or improper queries which were not reasonably likely to return foreign intelligence information due to their design. Regardless of United States person status, robust oversight is conducted to ensure compliance with all aspects of the targeting and minimization procedures; all identified incidents are reported to the FISC and to the Congress, and all incidents are required to be appropriately remedied. As with all incidents, the joint oversight team works closely with NSA to identify causes of incidents in an effort to prevent future incidents, regardless of United States person status.

(U) In the subsections that follow,<sup>65</sup> this joint assessment examines some of the underlying causes of incidents of non-compliance. This joint assessment first begins by examining and explaining incidents impacting United States persons' privacy interests, even though those incidents represent a minority of the overall incidents, followed by a discussion of other types of human errors and communication issues.

#### **(U) A. The Impact of Compliance Incidents on United States Persons**

(U) A primary concern of the joint oversight team is the impact of certain compliance incidents on United States persons.<sup>66</sup> United States persons were primarily impacted by (1) tasking errors that led to the tasking of facilities used by United States persons, and (2) delays in detasking facilities after NSA learned that the user of the facility was a United States person. United States persons were also impacted by minimization and querying errors during this reporting period, which are detailed below. While the number of incidents involving United States persons remains low, due to their importance, these incidents are highlighted in this subsection.

---

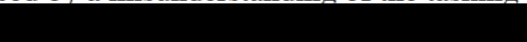
<sup>65</sup> (U) Although ODNI and DOJ strive to maintain consistency in the headings of these subsections, these headings may change with each joint assessment, depending on the incidents that occurred during that reporting period and the respective underlying causes.

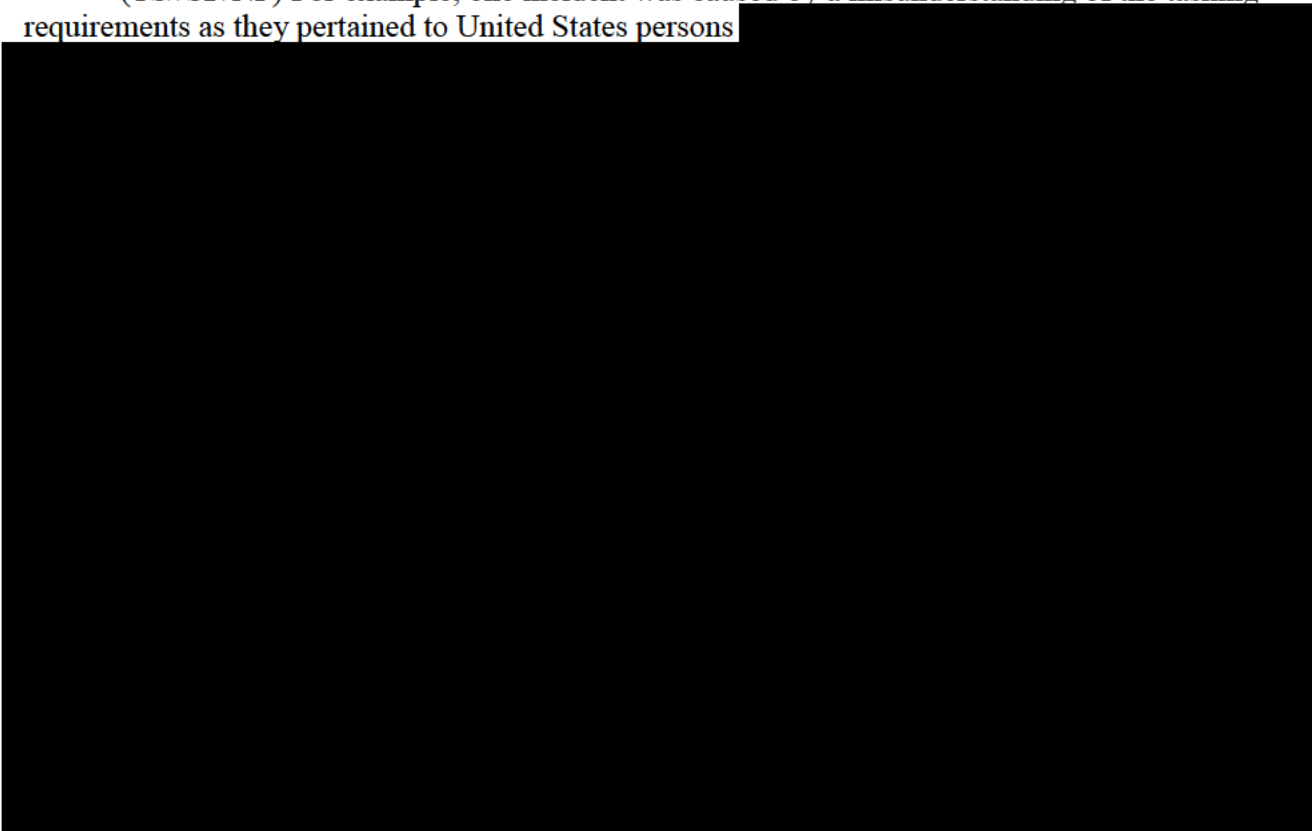
<sup>66</sup> (U) The Section 707 Report discusses every incident of non-compliance with the targeting, minimization, and querying procedures and how any erroneously acquired, disseminated, or queried United States person information was remediated through various purge, recall, and deletion processes.

~~TOP SECRET//SI//ORCON/NOFORN~~

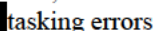
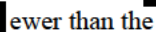
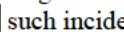

~~TOP SECRET//SI//ORCON//NOFORN~~*(U) (1) Tasking Errors Impacting United States Persons*

(U) ~~(S//NF)~~ During this reporting period, 4.1 percent of the total number of tasking errors identified involved instances where facilities used by United States persons were tasked pursuant to Section 702.<sup>67</sup> This percentage represents a slight increase from the last reporting period. All of the tasking errors in this reporting period impacting United States persons involved the tasking of facilities where the Government knew or should have known that at least one user of the facility was a United States person. These incidents represent isolated instances of insufficient due diligence, or other oversights, and did not involve an intentional effort to target a United States person. The majority of these tasking errors involved situations where an analyst made an erroneous assessment, overlooked information, and/or conducted insufficient research prior to tasking a facility and, as a result, inadvertently tasked a facility used by a United States person. In all of the incidents, personnel were reminded of the Section 702 tasking requirements, use of any applicable collection was restricted in NSA's systems, and any applicable collection was purged as required by NSA's targeting and minimization procedures.

~~(TS//SI//NF)~~ For example, one incident was caused by a misunderstanding of the tasking requirements as they pertained to United States persons 



---

<sup>67</sup> ~~(S//NF)~~ Note that this is 4.1 percent of tasking errors. As described above, the overall tasking compliance incident rate involving United States persons was close to zero. There were  tasking errors during this reporting period that involved facilities used by United States persons.  fewer than the  such incidents in the prior reporting period. 

<sup>68</sup> 

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(U) (2) *Delays in Detasking Impacting United States Persons*

(U) During this reporting period, 4.9 percent of detasking delays involved facilities used by a United States person. This percentage represents a slight decrease from the last reporting period.<sup>69</sup> The detasking delay incidents impacting United States persons in this reporting period were caused by unintentional human errors (such as misunderstandings of the detasking requirements or instances of poor interagency communication). One such detasking delay is described above because it involved both a tasking error and a detasking delay. In all of the incidents, personnel were reminded of the Section 702 tasking requirements, any applicable collection was purged, and no reporting was identified based on the collection.

(U) **B. Effect of Human Error**

(U) Unlike in the immediately prior section, which focused exclusively on incidents impacting United States persons, this section addresses incidents that impacted *both* United States persons and non-United States persons. Each of the agencies has established processes to both reduce human errors and to identify such errors when they occur. Some human errors, such as those resulting from misunderstanding the rules and procedures, can be mitigated with additional training and guidance. These processes and trainings have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated.

(U) (1) *Tasking & Detasking Errors*

(U) This section discusses some of the common types and causes of tasking errors and detasking delays from this reporting period, along with the corresponding compliance trends.<sup>70</sup> The majority of the detasking delays during this reporting period involved (i) non-United States persons who either traveled to the United States or appeared to have traveled to the United States, or (ii) unexplained indications that a Section 702-tasked account appeared to have been accessed from within the United States.

- (U) “Foreignness determination” errors – Certain tasking errors result from NSA not properly establishing a sufficient basis to assess that a target was located outside the United States (otherwise referred to as the “foreignness determination”) or not sufficiently addressing conflicting information that calls into question whether a target was located outside the United States. During this reporting period, approximately 23 percent of tasking errors were the result of insufficient foreignness determinations, an

---

<sup>69</sup> ~~(S//NF)~~ Note that this is approximately 4.9 percent of detasking incidents. As described above, the overall detasking compliance incident rate involving United States persons was close to zero. There were [REDACTED] detasking delays in this reporting period that involved facilities used by United States persons. [REDACTED] This is [REDACTED] in the prior reporting period.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

increase from the previous reporting period's 12 percent.<sup>71</sup> Certain of these incidents involved the failure to conduct a necessary foreignness check prior to tasking, or involved too long of a delay between the necessary foreignness checks and the tasking of the facility. In many of these incidents, NSA advised that it acquired no data from the erroneous tasking. However, in the instance data was acquired, it was purged.

- (U) “Foreign intelligence information purpose” errors – Certain tasking errors result from NSA's failure to establish a valid “foreign intelligence information purpose” for the tasking (*i.e.*, that the targeted user is not reasonably expected to possess or receive, and/or is not likely communicate foreign intelligence information as defined in 50 U.S.C. § 1801(e)) in relation to the categories of foreign intelligence information specified in the Section 702 certifications. During this reporting period, approximately 16 percent of tasking errors were the result of NSA not having a sufficient foreign intelligence purpose for the tasking, an increase from the previous reporting period's 11 percent.<sup>72</sup> In all of the instances, at the time of tasking, NSA had sufficiently established that the users were non-United States persons located outside the United States. Any erroneously collected information was purged, and no reporting was identified.
- (U) Typographical errors – Certain tasking errors result from typographical or similar errors. During this reporting period, approximately 21 percent of the tasking errors involved typographical or similar errors, a decrease from the previous reporting period's 39 percent. The majority of these errors were caused by CIA. In all but one of the incidents, NSA advised that there was no indication that the incorrectly tasked facilities were used by a United States person or by someone in the United States.<sup>73</sup> NSA and CIA advised that each had completed any required purges.
- (U) Incorrect providers – Certain tasking errors result from NSA inadvertently tasking a facility to an incorrect provider. During this reporting period, 3 percent of tasking errors involved tasking a facility to an incorrect provider, a slight decrease from the previous reporting period's 4 percent. Each of NSA, CIA, and FBI advised that it completed any required purges, and that it has identified no reporting based on this collection.
- (U) Incomplete Detaskings – Certain detasking delays result from NSA detasking (or another agency requesting that NSA detask) some, but not all, of a target's facilities. During this reporting period, 22 percent of the detasking delays involved such incidents where certain of a targets facilities were not timely detasked, an increase from the prior reporting period's 15 percent. Again, any data acquired as a result of such detasking errors was purged.

71

72

73

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

- (U) Facilities that Do Not Exist – In addition, during this reporting period, approximately 10 percent of the detasking delays were the result of the relevant provider indicating that a tasked facility did not exist, but NSA did not promptly detask the facility. One such incident involved a potentially widespread misunderstanding of NSA’s targeting procedures.<sup>74</sup> Specifically, while investigating an unrelated matter, NSA discovered that certain NSA analysts may not have understood their responsibilities with respect to Section 702-tasked facilities that providers have indicated do not exist. In March 2020, NSA issued revised guidance to its personnel to address the relevant misunderstanding and implemented changes to its systems to mitigate the likelihood of these types of incidents reoccurring.

(U) (2) *Minimization and Querying Errors*

(U) NSA’s minimization procedures have various requirements, including rules regarding under what circumstances Section 702-acquired information may be *disseminated*, and rules regarding how long unminimized Section 702-acquired information may be *retained*. NSA’s querying procedures also have various requirements, including rules regarding *querying* unminimized Section 702-acquired information. Particular issues of non-compliance with minimization and querying procedures are detailed below.

(U) Querying Rules: During this reporting period, NSA’s querying procedures included two principle restrictions on querying unminimized Section 702 collection.

- 1) NSA’s Section 702 querying procedures in effect during this reporting period required that queries of unminimized Section 702 collection *must be designed in a manner “reasonably likely to return foreign intelligence information.”* For example, if a query does not meet this standard due to a typographical or comparable error in the construction of the query term,<sup>75</sup> it constituted a compliance incident, regardless of whether the query term used a non-United States person identifier or a United States person identifier.
- 2) Although NSA’s Section 702 querying procedures in effect during this reporting period permitted queries of unminimized Section 702 content using United States person identifiers, such queries *must be approved by NSA OGC*. If an NSA analyst used a United States person identifier that had not been approved by NSA OGC to query Section 702-acquired data, it constituted a compliance incident.

(U) During this reporting period, NSA minimization and querying incidents accounted for 23 percent of all NSA incidents of noncompliance, as compared to 29 percent in the previous reporting period; during this reporting period, there was also a significant decrease in the number of minimization and querying incidents.<sup>76</sup>

<sup>74</sup> [REDACTED]

<sup>75</sup> (U) For example, this type of query error occurs when an analyst mistakenly inserts an “or” instead of an “and” in constructing a Boolean query, resulting in an improperly tailored query that would potentially receive overly broad results and was unlikely to retrieve foreign intelligence information.

<sup>76</sup> ~~(S//NF)~~ Minimization and querying incidents decreased to [REDACTED] incidents in the previous reporting period.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(U) As with prior joint assessments, query incidents remain the cause of most compliance incidents involving NSA's minimization and querying procedures. In the previous reporting period, approximately 88 percent of incidents of noncompliance with NSA's minimization and querying procedures involved improper queries. During this reporting period, out of all of NSA's minimization and querying errors, approximately 91 percent involved improper queries, of which:

- Approximately 55.3 percent of the minimization and querying errors involved queries that were not reasonably likely to return foreign intelligence information,<sup>77</sup> which represents an increase from the previous reporting period's 50.1 percent. However, while the percentage of the total increased, the actual number of queries that were not reasonably likely to return foreign intelligence information decreased during this period. Some of the errors were caused by NSA analysts incorrectly formatting a query or conducting a query without sufficient limiting criteria; other errors were caused by analysts using identifiers with an insufficient connection to a Section 702 target or to a foreign intelligence purpose.<sup>78</sup> NSA advised that the relevant personnel had been reminded of the query requirements and that all query results had been deleted or aged-off.
- Approximately 35.5 percent of the minimization and querying errors involved NSA analysts conducting queries using a United States person identifier without approval, which represents a slight decrease from last reporting period's 38.6 percent (the actual number of such queries also decreased during this reporting period).<sup>79</sup>

(U) The joint oversight team assesses that NSA's overall training and guidance to its personnel has contributed to its overall compliance with its querying procedures, although individuals continue to make mistakes. The joint oversight team has reviewed the human errors that caused the minimization and querying errors during this reporting period and has not identified any discernible patterns in the types or causes of these errors.

(U) As with previous reporting periods, there were no identified NSA incidents of an analyst intentionally running improper queries.

<sup>77</sup> ~~(TS//SI//NF)~~ There were [REDACTED] such non-compliant queries during this reporting period, compared to [REDACTED] in the previous reporting period.

<sup>78</sup> [REDACTED]

<sup>79</sup> ~~(TS//SI//NF)~~ There were [REDACTED] United States person query incidents involving NSA during this reporting period, compared to [REDACTED] in the previous reporting period. All [REDACTED] incidents involved NSA analysts using United States person identifiers that had not been approved to query Section 702-acquired data. In one example, [REDACTED]

[REDACTED] had not been approved as query terms in accordance with NSA's Section 702 querying procedures. NSA advised that the relevant personnel have been reminded of the Section 702 query requirements.

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

(U) Dissemination Rules: NSA's minimization procedures set forth requirements for the dissemination of United States person information. In the current reporting period, incidents involving NSA's dissemination of United States person information that did not meet the dissemination standard in NSA's minimization procedures represented approximately 8 percent of the total number of minimization and querying incidents (compared to 9 percent of minimization and querying incidents during the last reporting period).<sup>80</sup> Improper disseminations of United States person information are usually the result of a human error oversight, generally because United States person information that is not necessary to understand foreign intelligence information is included in the dissemination. For example, in one instance, NSA issued a report on September 4, 2019, that included the name of a United States person whose identity was not necessary to understand foreign intelligence information. The error occurred because an NSA analyst had attempted to redact the United States person identity in the report by using a particular feature in a software tool. However, based on the way the software tool was utilized, it was possible for recipients to remove the redaction and view the United States person identity. NSA recalled the report and did not reissue it. NSA advised that the relevant personnel have been reminded of the Section 702 dissemination requirements. In another instance, the error occurred because disseminations of United States person information were distributed to a broader group of recipients than is permitted by NSA's minimization procedures. The joint oversight team has reviewed the human errors that caused the dissemination errors during this reporting period and has not identified any discernible patterns in the types or causes of these errors.

(U) As was the case with NSA querying incidents, there were no identified NSA incidents of an analyst intentionally violating the dissemination rules.

~~(TS//SI//NF)~~ Retention Rules: During this reporting period, there were [REDACTED] incidents in which NSA improperly retained information acquired pursuant to Section 702, either because it should have been purged or because it was retained longer than permitted by NSA's minimization procedures.<sup>81</sup> These incidents primarily involved NSA system errors, including human errors in system coding. For example, NSA discovered that FISA information subject to purge was improperly retained in an NSA system [REDACTED]

[REDACTED] NSA has deleted the improperly retained records [REDACTED]

<sup>80</sup> ~~(S//NF)~~ There were [REDACTED] incidents involving NSA's dissemination of United States person information that did not meet the dissemination standard in NSA's minimization procedures, compared to [REDACTED] in the previous reporting period.

<sup>81</sup> ~~(TS//SI//NF)~~ There were [REDACTED] incidents involving the retention of unminimized Section 702-acquired data beyond the period permitted by NSA's Section 702 minimization procedures, and [REDACTED] incidents involving the failure to conduct post-targeting analysis, as required by the targeting procedures

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

(U) (3) *Other Errors*<sup>82</sup>

(U) Documentation Errors: NSA's targeting procedures require that for each tasked facility NSA document the source of the "foreignness determination" and identify the foreign power or foreign territory about which NSA expects to obtain foreign intelligence information. The targeting procedures also require a written explanation of the basis for its assessment, at the time of targeting, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning the foreign power or foreign territory that is covered by the certification under which the accounts were tasked ("foreign intelligence purpose"). The number of documentation errors increased to approximately 30.1 percent of the total number of compliance incidents in this period, from 14.7 percent in the prior reporting period.<sup>83</sup> In all of these incidents, while the actual tasking of each facility was appropriate, the analyst failed to sufficiently document the "foreignness determination" or the "foreign intelligence purpose" on the tasking sheet, or the Section 702(h) certification to which the facility was tasked was not appropriate based on the documented foreign intelligence purpose. In each of these incidents, NSA issued reminders to the targeting officer to review the tasking sheet data thoroughly prior to submission and to select the appropriate certification based on the foreign intelligence they expected to receive from the user.

(U) Notification Delays: Notification errors remained relatively high, accounting for 19 percent of all NSA compliance incidents in this reporting period, a slight increase from 18 percent in the last reporting period.<sup>84</sup>

~~(TS//SI//NF)~~ Post-Targeting Analysis: NSA's targeting procedures require that "After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis . . . designed to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States is located in the United States." During this reporting period, there were [REDACTED] incidents involving the failure to satisfy the requirements for post-targeting analysis in NSA's targeting procedures.

<sup>82</sup> ~~(TS//SI//NF)~~ In addition to the incidents discussed below, there was one incident involving NSA's failure to purge Section 702-acquired information that was required to be purged pursuant to NSA's Section 702 targeting procedures. There were also [REDACTED] incidents involving NSA analysts improperly storing or accessing Section 702-acquired data.

<sup>83</sup> ~~(S//NF)~~ [REDACTED] incidents resulted from documentation errors, representing an increase from the last reporting period, [REDACTED]. The number of documentation errors resulting from the tasking of a facility to a different DNI/AG Section 702(h) certification than intended remained high but decreased [REDACTED] in the prior reporting period.

<sup>84</sup> ~~(TS//SI//NF)~~ There were [REDACTED] reporting delays in this reporting period. In [REDACTED] of the incidents, the only violation was a failure to provide the required notice to NSD. These reporting delays ranged from one to 148 business days, with an average delay of approximately six business days and a median delay of approximately two business days.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

### (U) C. Inter-Agency and Intra-Agency Communications

(U) Section 702 compliance requires good communication and coordination within and between agencies. In order to ensure targeting decisions are made based on the totality of the circumstances and after the exercise of due diligence, those involved in the targeting decision must communicate the relevant facts to each other. Analysts also must have access to the necessary records that inform such decisions. Good communication among analysts is needed to ensure that facilities are promptly detasked when it is determined that the Government has lost its reasonable basis for assessing that the facility is used by a non-United States person reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Furthermore, query rules regarding United States person identifiers and dissemination decisions regarding United States person information require inter- and intra-agency communications regarding who the Government has determined to be a United States person.

(U) In this reporting period, approximately 14.6 percent of the detasking delays were attributable to miscommunications or delays in communicating relevant facts.<sup>85</sup> This is similar to the last reporting period (15 percent) and, thus, the joint oversight team assesses that there is still room to improve agency communication. The detasking delays caused by miscommunication typically involved travel or possible travel of non-United States persons to the United States. Further, none of the tasking errors involved situations in which intra-agency miscommunications resulted in the erroneous tasking of a facility.

(U) The joint oversight team assesses that agencies should continue their training efforts to ensure that appropriate protocols continue to be utilized. As part of its ongoing oversight efforts, the joint oversight team will also continue to monitor NSA, CIA, FBI, and NCTC's Section 702 activities and practices to ensure that the agencies maintain efficient and effective channels of communication.

### (U) III. Review of Compliance Incidents – FBI Targeting, Minimization, and Querying Procedures

(U) There was a significant decrease in the number of incidents involving noncompliance with FBI's targeting, minimization, and querying procedures. However, as with the previous reporting period, a large majority of those incidents involved querying errors.<sup>86</sup> Most of the querying incidents were caused by personnel misunderstanding the application of the query standard in the context of batch queries.

---

<sup>85</sup> ~~(S//NF)~~ There were [REDACTED] such incidents in this reporting period, a slight reduction from the [REDACTED] reported in the previous period. [REDACTED]

<sup>86</sup> ~~(S//NF)~~ As noted above, [REDACTED] compliance incidents involved violations of FBI's targeting, minimization, or querying procedures. The substantial decrease is likely due in part to the suspension of NSD's minimization and querying reviews at FBI field offices, and in part to FBI's efforts to provide training and resources to reduce query errors. Out of the total FBI compliance incidents for this reporting period, only [REDACTED] were targeting errors, [REDACTED] were minimization errors, and the remaining [REDACTED] were querying errors.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~**(U) A. Targeting Incidents**

~~(S//NF)~~ During this reporting period, there were [REDACTED] incidents involving non-compliance with FBI's targeting procedures, [REDACTED] from the previous reporting period.<sup>87</sup> In all [REDACTED] cases, FBI personnel approved a request to [REDACTED] from a Designated Account prior to completing all searches of FBI systems required by FBI's targeting procedures. In all [REDACTED] incidents, FBI conducted additional searches after the review and advised that it had no information indicating that the Designated Accounts were used by a United States person or by someone located in the United States, thus, the accounts remained tasked. In all of the incidents, FBI personnel were reminded of the Section 702 requirements for tasking, including completing all the required searches in FBI systems.

**(U) B. Minimization and Querying Incidents**

(U) With respect to FBI's minimization and querying procedures, the total number of compliance incidents decreased substantially from the previous reporting period.<sup>88</sup> As discussed above, the joint oversight team believes that the reduction in compliance incidents is, in part, due to the suspension of reviews at FBI field offices.<sup>89</sup> In addition to discussing the query incidents, this assessment discusses other errors involving noncompliance with FBI's minimization procedures. Details about remedial actions are provided below.

**(U) (1) Batch Query Errors**

(U) During prior reporting periods, NSD identified noncompliant batch queries conducted by FBI personnel that resulted in thousands of noncompliant queries due to a single decision by a user. During this reporting period, NSD identified a batch job involving queries of large numbers of identifiers, including United States person identifiers, without having a reasonable expectation that such queries were likely to return foreign intelligence information or evidence of a crime. Because certain FBI systems permit users to conduct multiple queries as part of a single batch job, a single action can result in thousands of improper queries. For example, if a user wanted to conduct a query based on 100 e-mail accounts that had been in contact with a FISA target, the user could use the batch query tool, which would result in 100 queries being conducted using each e-mail account as a query term. In these incidents, although the FBI analysts conducted the queries for work-related purposes, such as attempts to investigate threats, the analysts misunderstood the application

---

<sup>87</sup> [REDACTED]

<sup>88</sup> ~~(S//NF)~~ The number of minimization and querying errors for the current reporting period was [REDACTED] compared to [REDACTED] in the previous reporting period.

<sup>89</sup> (U) In response to the coronavirus pandemic, NSD and ODNI temporarily suspended reviews at FBI field offices during a portion of this reporting period. In recent years, these field office reviews had been responsible for discovering a significant portion of FBI's minimization and querying incidents that are reported in each Section 707 Report. As a result, incidents that would typically be discovered by NSD during those field office reviews were not discovered during the portion of this reporting period when such reviews had been suspended. FBI's minimization and querying incidents discussed in this joint assessment were first reported to the FISC during this reporting period, but certain of those incidents were discovered in connection with field office reviews conducted during prior reporting periods. In February 2021, NSD resumed its audits of queries conducted by FBI personnel; these audits are being conducted remotely due to the pandemic. Any incidents discovered will be discussed in future joint assessments.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

of the query requirements. Thus, as the FISC explained in its October 2018 opinion, “a single improper decision or assessment resulted in the use of query terms corresponding to a large number of individuals, including U.S. persons.”

~~(S//NF)~~ Approximately 37 percent of all FBI compliance incidents during this reporting period were the result of a single improper querying decision.<sup>90</sup> Specifically, an FBI intelligence analyst (IA) conducted approximately [REDACTED] queries in [REDACTED] using the names and other identifiers of individuals, including United States persons, whom FBI had identified as potential sources because they were linguists who had applied to work at FBI but were not ultimately hired. The IA advised that she conducted these queries in order to find out whether FBI had any derogatory information about these individuals, which would assist FBI in deciding whether or not to approach the individuals as potential sources. The IA further advised that, prior to conducting these queries, she had no reason to suspect that any of the queries would return foreign intelligence information or evidence of a crime. The IA indicated that she had conducted these queries as a result of an initiative directed from an FBI Headquarters component to FBI field offices, and NSD is aware of at least one other field office where similar queries were conducted.

~~(S//NF)~~  
(U) Although reported to the FISC during this reporting period, the underlying batch error that caused these incidents was conducted earlier in 2019, prior to a number of remedial steps taken by FBI in late 2019, 2020, and 2021. For example, to address these types of batch query compliance incidents where a single improper decision or assessment by FBI personnel results in noncompliant queries corresponding to a large number of individuals, FBI (subsequent to this reporting period) imposed a requirement that individual queries conducted using the batch query tool in [REDACTED] of 100 or more identifiers require FBI attorney approval prior to the queries being conducted. This change became effective in [REDACTED] as of June 2021. Further remedial steps applicable to all queries, including batch query incidents, are discussed in a subsection below.

#### (U) (2) *Other Query Errors Caused by Misunderstandings of the Query Standard*

(U) During this reporting period, after batch queries are removed, most of the improper query incidents resulted from FBI personnel misunderstanding the querying rules even though the queries were conducted for work-management purposes or work-related purposes. These queries were not, however, reasonably likely to retrieve foreign intelligence information or evidence of a crime and, thus, constituted incidents. In most of the instances, FBI personnel did not fully understand the application of the query rules; however, it appears that in at least one instance, FBI personnel explained that they did not recall why they ran the query.

(U) For example, some of the improper queries involved FBI personnel conducting queries, including using United States person identifiers, to research prospective FBI employees without a reasonable basis to believe the queries would be likely to return foreign intelligence information or evidence of a crime.<sup>91</sup> These and other similar query compliance incidents during this period were

---

<sup>90</sup> ~~(S//NF)~~ The largest single FBI compliance incident involved [REDACTED] improper batch queries of unminimized FISA-acquired information in [REDACTED]. [REDACTED]

<sup>91</sup> ~~(S//NF)~~ In one incident, an FBI operational support technician conducted approximately [REDACTED] queries in [REDACTED] using identifiers associated with task force officers who were FBI bomb technician candidates and close personal contacts

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

due to personnel conducting queries to vet individuals or entities for any derogatory information. NSD has observed this common scenario in numerous query compliance incidents in this and prior and subsequent reporting periods. These types of queries can impact United States persons. For this category of incidents, NSD has concluded that there is no specific factual basis, absent additional information, to believe that the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime from raw FISA collection, and, therefore, the queries do not meet the justification component of the querying standard.

~~(S//NF)~~ During this reporting period, NSD observed multiple query incidents involving FBI looking for derogatory information about individuals. For example, in one review NSD conducted, NSD identified [REDACTED] query compliance incidents involving three categories of individuals. The first category consisted of individuals who had been subjected to a limited background investigation because they had requested to participate in FBI's "Citizens Academy" – a program for business, religious, civic, and community leaders designed to foster a greater understanding of the role of federal law enforcement in the community through discussion and education, according to FBI's website. Candidates are nominated by FBI employees, former Citizens Academy graduates, and community leaders, and participants are selected by the special agent in charge of the local FBI field office. The second category consisted of individuals who had been subjected to a limited background investigation because they needed to enter the field office in order to perform a particular service, such as a repair. The third category (referred to as "walk-in complaints") consisted of individuals who entered the field office seeking to provide a tip or to report that they were the victim of a crime. The technical information specialist advised that he conducted these queries in order to determine whether FBI had any derogatory information regarding the individuals. In another example, NSD's audits revealed that FBI personnel conducted queries of individuals whom FBI was considering approaching as sources, [REDACTED]. In addition, the batch query incident discussed above was run for the same purpose of vetting individuals to determine if there was any derogatory information in FBI holdings.

(U) ~~(S//NF)~~ In one query incident, FBI queried the names of a local political party to determine if the party had connections to foreign intelligence. This query was not reasonably likely to retrieve foreign intelligence information.

(U) In addition, NSD's query audits revealed noncompliant queries of complainants who provided tips to the FBI. FBI personnel also conducted queries that, while reasonably likely to return foreign intelligence information, were overly broad as constructed.<sup>92</sup> In all of the above

---

reported by other FBI personnel; the queries were conducted to determine if there was any derogatory information about these individuals. [REDACTED] The FBI employee who conducted the query advised that, to the best of her knowledge, the queries did not return any unminimized FISA-acquired information.

<sup>92</sup> ~~(S//NF)~~ An IA conducted approximately [REDACTED] queries in [REDACTED] using only the name of a U.S. congressman. [REDACTED] The 707 Report describes the specific facts that led the IA to conduct these queries. These queries retrieved unminimized FISA-acquired information, including Section 702-acquired products that were opened. FBI advised that no unminimized FISA-acquired information was disseminated or used in any other way. NSD and ODNI assess, based on these facts, that these queries were not compliant because they were overly broad as constructed (*i.e.*, queried the U.S. congressman's name with no limiters).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

incidents, FBI personnel misunderstood the application of the query rules, and they were subsequently reminded of how to correctly apply the query rules.

*(U) (3) Other Query Errors Caused by Lack of Awareness that a Query Would Run against FISA-Acquired Data*

(U) In other incidents, FBI personnel advised that they did not appreciate that queries would be running against unminimized FISA-acquired information and, thus, would be subject to the query standard. This is particularly the case with respect to query incidents that have been identified with queries run in a specific FBI database that contains non-FISA acquired and unminimized FISA-acquired information. As a result, for these queries, FBI personnel did not think to apply the query standard to their proposed queries before conducting queries in that particular FBI database, or failed to opt out of conducting queries against unminimized FISA-acquired information.

~~(S//NF)~~ A change that FBI has (subsequent to this reporting period) implemented to make [REDACTED] a default opt-out for searches of FISA-acquired information is designed to prevent this type of incident. At the time these queries were conducted, [REDACTED] was configured to automatically include FISA datasets – including data acquired pursuant to Titles I, III, and V as well as Section 702 of FISA – and any other datasets the user was authorized to access unless personnel intentionally excluded such data. Pursuant to a change FBI has implemented, a user will now have to intentionally decide to opt-in to unminimized FISA datasets if the user wants to query those datasets. This change to [REDACTED] became effective on 29 June 2021.

*(U) (4) Errors related to Queries Conducted Solely for an Evidence of a Crime Purpose*

~~(S//NF)~~ Additionally, there were [REDACTED] incidents involving violations of the requirement<sup>93</sup> that the Government promptly submit in writing a report concerning each instance in which FBI personnel receive and review Section 702-acquired information that FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information.<sup>94</sup> Further, Section 702(f)(2)(A) provides that FBI may not access the contents of communications acquired pursuant to Section 702 that were retrieved pursuant to a query made using a United States person query term that was not designed to find and extract foreign intelligence information unless FBI applies for an order from the FISC, based on probable cause, and the FISC enters an order approving the application. In these instances, NSD determined that these queries had been conducted solely to find and extract evidence of a crime as part of predicated criminal investigations. The [REDACTED] incidents were discovered by NSD while conducting oversight reviews at five FBI field offices. Of the [REDACTED] incidents, [REDACTED] occurred at one field office, many of which related to public corruption or embezzlement investigations unrelated to foreign intelligence activity. Subsequent investigation by FBI into these queries revealed that they returned Section 702-acquired information, and NSD presumed that such information was reviewed by FBI

---

<sup>93</sup> (U) This requirement is not contained in FBI's querying procedures. Rather, it is contained in each of the FISC's opinions approving the relevant annual certifications, beginning with the November 6, 2015 Opinion and Order approving the 2015 FISA Section 702 Certifications.

<sup>94</sup> [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

personnel absent specific information to the contrary. The system that was involved with these particular incidents was configured, at the time of the incidents, to preview content of responsive information for users when they executed a query.<sup>95</sup> Subsequent to when these queries were conducted, FBI reconfigured the system at issue so that it no longer presents a preview of the content of unminimized Section 702-acquired information in response to a query. The users who executed these queries were unaware of the particular requirements of Section 702(f)(2), and of an option provided by the system to indicate that their queries were being run solely to extract evidence of a crime in support of a predicated criminal investigation. Because the queries were run using United States person query terms in order to find and extract evidence of a crime in support of predicated criminal investigations, and because NSD had to presume, because of this system design issue, that FBI personnel reviewed the Section 702-acquired information without first obtaining an order from the FISC, NSD reported these incidents to the FISC as potential violations of Section 702(f)(2)(A) of FISA. In these incidents, NSD reminded the personnel about the query requirements in FBI's Section 702 query procedures and FBI's FISA minimization procedures, and discussed these requirements with other personnel during NSD's training conducted for the field offices.

(U) In addition, to the reconfiguration of the system at issue as noted above, if the user seeks to access Section 702-acquired content returned from a query, the system will force the user to complete the query in another FBI system. That other FBI system requires the user to answer a question in a pop-up box that asks whether the query is being done only to retrieve evidence of a crime. An information icon also is provided, providing the user with information relating to the requirements of Section 702(f)(2) of FISA. FBI designed the radio buttons, however, to automatically default the answer to this question in the system to "No." If a user proceeds from that default "No," they are able to select from a series of pre-populated justifications for their query, or select "other" and provide their own, written justification. Once the system receives that justification from the user, it allows the user to access the contents of the Section 702-acquired information. If, however, the user answers "Yes" to the question as to whether it is a query being done to retrieve evidence of a crime, the user is provided with three drop-down justifications for their query: "Court Order," "Exigent Circumstances," or "Neither." If a user selects "Court Order" or "Exigent Circumstances," she is allowed to proceed to access the contents of the Section 702-

---

<sup>95</sup> ~~(S//NF)~~ For queries in █████ during the reporting period, although FBI was able to confirm whether or not a user reviewed the contents of Section 702-acquired information returned by a query (e.g., by opening the product(s) containing the Section 702-acquired information), the manner in which █████ was configured did not allow FBI to confirm whether a user was exposed to content that is previewed for the user on their computer screen in response to a query. With limited exceptions involving highly sensitive collections, query results returned to a █████ user would have generally included a 100 character context (or summary) field for each search result, which could include information from FISA-acquired products. When presented, this summary field consists of the 100 characters surrounding the individual search "hit" (e.g., the query term) within the individual product. As a result, a █████ user could be exposed to FISA-acquired information in response to a query without actually clicking on the actual FISA-acquired product. Further, individual █████ users have the ability to customize the number of search results that appear on each screen page that the query returns (e.g., 25, 50, 100 results per page) and have the ability to change those preferences at any time. During the reporting period, █████ was not designed to log how far down a user scrolls through search results on an individual screen, or to automatically report how many, or which, pages of search results an individual user clicks through. Accordingly, without any additional information (e.g., the user remembers not reviewing the query results or the user set up his/her user preferences to not have the summary field displayed when the query results are returned), NSD presumed that the users would have viewed the content of the 702-acquired information in the summary field.

~~TOP SECRET//SI//ORCON//NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~

acquired information. At that same time, an alert is sent to FBI's NSCLB, which then conducts additional research into the nature of the query, and coordinates as necessary with NSD. If the user selects "Neither," she is prevented from accessing the contents of the Section 702-acquired information, and provided with an alert that instructs her that she either needs to obtain an order from the FISC or have exigent circumstances to be able to review the contents of the Section 702-acquired information. This alert also directs the user to contact NSCLB or her field office Chief Division Counsel with any questions. Although outside this reporting period, the FBI changed the system design pertaining to the question of whether the query is being done only to retrieve evidence of a crime. The system has now been reconfigured to eliminate a default answer, so that FBI personnel must affirmatively indicate whether or not a query is being conducted solely to retrieve evidence of a crime before they may proceed to conduct a query.

*(U) (5) Errors related to Queries Conducted in Connection with National Security Assessments*

(U) In addition to the minimization reviews conducted by NSD described above in Section II, NSD also conducted NSRs at FBI field offices during this reporting period. As noted above, during an NSR, team members review, among other things, a sampling of each office's national security assessments to verify that they were opened for an authorized purpose – that the basis for the assessment was not arbitrary or groundless speculation, nor based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin, or religion of the subject. *See generally* Attorney General Guidelines for Domestic Operations (AGG-DOM) at 10, 13, 16-19, Section II. While FBI personnel may query FBI systems containing unminimized Section 702 data as part of an assessment, any queries involving assessments that lacked an authorized purpose would necessarily be improper, as such queries would not be reasonably likely to return foreign intelligence information or evidence of a crime.

~~(S//NF)~~ During this reporting period, there were [REDACTED] improper queries conducted in connection with assessments that NSD determined lacked an authorized purpose. For example, in 2016 and 2017, an FBI analyst conducted queries related to an assessment opened based on a witness's report that a vehicle driven by an individual of Middle Eastern descent sped into the parking lot and began honking the horn. A second individual of Middle Eastern descent came out of the apartment complex, and the individuals began loading boxes into a second vehicle. The witness reported that some of the boxes were labeled "Drano," and that there were also "white containers which appeared to be upside down with black screw tops in the box." The witness stated that the individuals acted very quickly. As a result of a 2019 review that revealed the above, NSD assessed that these facts were insufficient to establish an authorized purpose for the assessment, and thus the [REDACTED] queries related to this assessment lacked a proper authorized purpose. In this instance, the assessment was closed at the time of NSD's oversight review. When NSD discovers closed assessments which lack an authorized purpose, it notes for FBI that any information obtained in the course of those assessments may have to be destroyed. The decision to destroy any such information is made on a case-by-case basis by FBI. Although the error in these assessments arose from a misapplication of the Attorney General Guidelines, as opposed to a misunderstanding of the FBI query procedures requirement for an authorized purpose, the joint oversight team will continue to closely monitor incidents such as these that may have particularly acute impacts on the privacy and civil liberties of United States persons.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(U) (6) *Other FBI Errors Caused by Misunderstanding or Lack of Awareness*

(U) During this reporting period, there were a modest number of incidents that involved non-compliance with the provisions of FBI's minimization procedures concerning establishment of a review team for a target charged with a crime pursuant to the United States Code.<sup>96</sup> As soon as FBI knows that a target is charged with such a crime, FBI's minimization procedures require that FBI follow certain steps, including establishing a review team of monitor(s). The member(s) of the review team must be individuals who have no role in the prosecution, and the monitor(s) initially assess and review the Section 702-acquired information to determine whether the communications are attorney-client privileged. Failure to timely establish such a review team constitutes a compliance incident. With respect to such incidents in this reporting period, the joint oversight team assesses that one set of incidents was the result of a misunderstanding of the process required to establish a review team, while the other set of incidents was the result of a miscommunication between the FBI division conducting the investigation and FBI Headquarters. In these incidents, the relevant personnel have been reminded about the requirements in FBI's Section 702 minimization procedures regarding attorney-client communications, including the review team requirements.

(U)

~~(S//NF)~~ Additionally, there was one incident where FBI personnel improperly disseminated United States person information acquired pursuant to Section 702.<sup>97</sup> The dissemination did not comply with section III.C.1.c, section IV.A, or section IV.B of FBI's Section 702 minimization procedures, in that the United States person information did not reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime.

(U) **C. Remedial Steps Taken to Address Query Errors**

(U) The joint oversight team has worked with FBI to address the query compliance issues through training, guidance, and system changes.

(U) *Historical Remedial Measures*

(U) For example, in June 2018, FBI, in consultation with the joint oversight team, issued guidance to all components where personnel had access to unminimized FISA-acquired information. This guidance explained the query standard and how to apply it. The guidance also discussed compliance issues involving the application of the query standard, including issues relating to queries run using the "batch" job function. Additional emphasis was provided concerning issues involving queries run against unminimized 702-acquired information to find and extract only evidence of a crime (and not foreign intelligence information). Each FBI field office was instructed to train their personnel on the June 2018 guidance. In January 2019, FBI and NSD conducted joint training for all FBI NSCLB personnel and all field office legal personnel, on FBI's querying procedures. FBI field office legal personnel were instructed to provide this training to all personnel with access to unminimized FISA-acquired information. In fall 2019, FBI, in

<sup>96</sup> [REDACTED]

<sup>97</sup> ~~(S//NF)~~ The relevant personnel were reminded about the requirements in FBI's Section 702 minimization procedures. [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

consultation with NSD, developed and deployed mandatory training for FBI personnel on the query standard and on the system changes FBI made to address the query issues. All personnel with access to unminimized FISA-acquired information were required to complete the training by mid-December 2019, and all personnel who subsequently require such access must first complete this training prior to being granted access. In addition, prior to the temporary suspension of NSD query audits in March 2020, NSD generally conducted query training during field office query audits. This training occurred during one on one sessions with the individuals being audited and as part of a larger group training at the field office. This training included, among other things, multiple hypothetical examples derived from actual query incidents, as well as guidance on how to use FBI's systems to allow FBI to better track and comply with requirements involving queries run against unminimized 702-acquired information.

(U) As part of FBI's Section 702 amended querying procedures that were adopted by the Attorney General in 2019, the amended procedures instituted recordkeeping and documentation requirements for United States person queries and, in response the FISC ordered the Government to periodically update the FISC on FBI's implementation of the new requirements. Between September and November 2019, FBI implemented changes to FBI systems storing unminimized FISA-acquired information that were necessary to comply with the amended procedures. Among other things, these changes require FBI personnel to provide a justification, explaining how their query meets the query standard when running queries of United States person query terms and when they seek to access Section 702-acquired contents returned by such queries. All query terms and justifications are logged for oversight purposes. In addition, FBI, in consultation with NSD, developed and deployed new training, as detailed above, for FBI personnel on the query standard and on the system changes.

*(U) Recent Training and Guidance*

(U) As noted above, in 2021, NSD resumed remote query audits of FBI users at multiple FBI field offices as well as FBI Headquarters. Those audits have sampled queries conducted in 2020 and 2021 and have revealed additional query compliance incidents. As a result of the findings from NSD's audits and observations of the FISC related to these query incidents, NSD, in consultation with ODNI, developed guidance on the query standard for FBI personnel. This guidance document is designed to supplement existing and planned training on the querying standard; provides a robust explanation of the query standard; and explains the specific requirements imposed by Section 702(f)(2). The guidance document also includes multiple examples of the application of the guidance to particular factual scenarios. On 01 November 2021, NSD provided this guidance document to FBI, and FBI will provide this guidance document to all users with access to raw FISA-acquired information. NSD anticipates that this additional guidance document will facilitate the correct application of the querying standard. Additionally, based on the above guidance regarding the querying standard, FBI is undertaking additional training for FBI personnel focused specifically on querying requirements in combination with the below-described changes to FBI's systems used to query unminimized Section 702-acquired information in order to more adequately address the query compliance issues. FBI plans to develop relevant training before the end of calendar year 2021. FBI will require all personnel with access to unminimized FISA-acquired information to verify that they have completed the required training.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~*(U) Recent Technical Changes*

(U) As detailed above, in June 2021, FBI took additional steps to address the batch query compliance incidents and instances where users do not intend to query unminimized FISA-acquired information but fail to opt-out of such datasets. In addition, FBI plans to redesign its systems that contain unminimized Section 702-acquired information to include a requirement that users write a case-specific justification for United States person queries that return Section 702 contents if they want to access the contents. Historically, users have been able to choose prepopulated justifications from a drop-down menu in lieu of entering a free text justification in certain circumstances. The joint oversight team assesses that user understanding of the querying standard can be enhanced if users are required to write their own case-specific justification for a Section 702 query in addition to choosing from a drop-down menu, because the user will be required to demonstrate that user's understanding of the querying standard. The joint oversight team also assesses that reviewing these case-specific justifications will enable both internal FBI overseers and external overseers at NSD and ODNI to better determine whether FBI personnel understand the querying standard. Because some of FBI's remedial measures did not come into effect until the end of June 2021, the joint oversight team, however, is unable, at this time, to assess the overall effectiveness of FBI's recent remedial measures, including the planned training and the recently issued guidance. The joint oversight team will provide updates on its assessment in future joint assessments.

**(U) IV. Review of Compliance Incidents – CIA Minimization and Querying Procedures**

(U) During this reporting period, there were a small number of incidents involving noncompliance with CIA's querying procedures.<sup>98</sup> All of these incidents involved queries of Section 702-acquired information that were not reasonably likely to retrieve foreign intelligence information.<sup>99</sup>

~~(S//OC/NF)~~ For example, [REDACTED]

[REDACTED] Despite this instruction, the analyst inadvertently designed the query to include CIA's 702 FISA collection. Although these queries returned unminimized 702-acquired information, the

<sup>98</sup> ~~(S//NF)~~ CIA receives unminimized communications from selectors that it nominates to NSA for targeting [REDACTED]

<sup>99</sup> ~~(S//NF)~~ There were [REDACTED] instances of noncompliance with CIA's querying procedures during the reporting period. In each of these incidents, CIA analysts queried the identifiers of subjects of various investigations, but the queries were not reasonably likely to return foreign intelligence information. [REDACTED]

100 [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

analyst advised that he/she did not disseminate or otherwise use any such information. CIA advised that the analyst at issue has been reminded of the requirements for querying United States person identifiers into Section 702-acquired content and to exercise care when performing these queries.

(U) **V. Review of Compliance Incidents – NCTC Minimization and Querying Procedures**

(U) During the reporting period, there were no incidents involving violations of NCTC’s minimization or querying procedures.

(U) **VI. Review of Compliance Incidents – Provider Errors**

(U) ~~(S//NF)~~ During the reporting period, there were no reported instances of non-compliance by a “specified person” (*i.e.*, a provider) to whom the Attorney General and DNI have issued directives pursuant to Section 702(i) of FISA.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~**(U) SECTION 5: CONCLUSION**

(U) During this reporting period, the joint oversight team found that the agencies continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. Nevertheless, a continued focus is needed to address the underlying causes of the incidents that did occur, especially those incidents relating to improper queries. The joint oversight team assesses that such focus should emphasize maintaining close monitoring of collection activities and continued personnel training. Additionally, as part of its ongoing oversight responsibilities, the joint oversight team and the agencies' internal oversight regimes will continue to monitor the efficacy of measures to address the causes of compliance incidents during the next reporting period.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

# APPENDIX

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

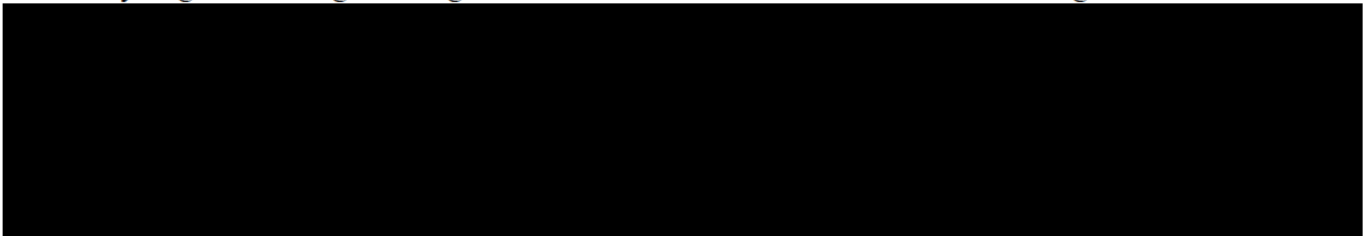
## APPENDIX

### (U) IMPLEMENTATION OF SECTION 702 AUTHORITIES – OVERVIEW

#### (U) I. Overview – NSA

(U) The National Security Agency (NSA) seeks to acquire foreign intelligence information concerning specific targets under each Section 702 certification from or with the assistance of electronic communication service providers, as defined in Section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA).<sup>1</sup> As required by Section 702, those targets must be non-United States persons<sup>2</sup> reasonably believed to be located outside the United States.

~~(S//NF)~~ During this reporting period, NSA conducted foreign intelligence analysis to identify targets of foreign intelligence interest that fell within one of the following certifications:



(U) As affirmed in affidavits filed with the FISC, NSA believes that the non-United States persons reasonably believed to be outside the United States who are targeted under these

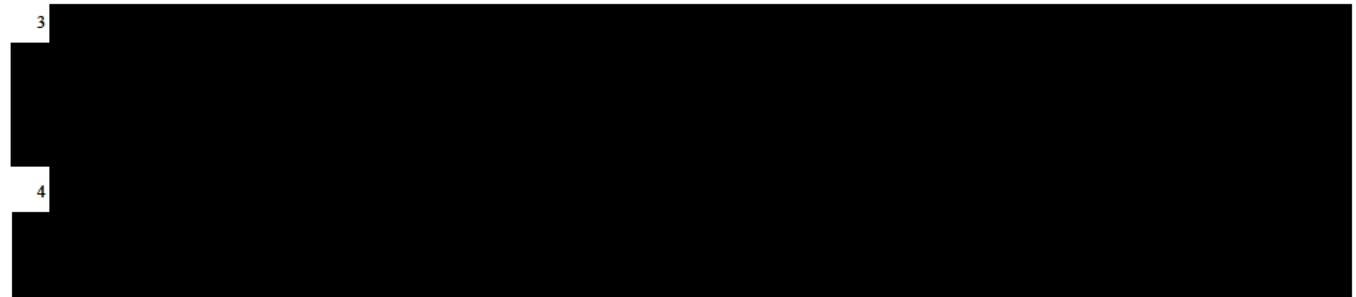
<sup>1</sup> (U) Specifically, Section 701(b)(4) provides:

The term ‘electronic communication service provider’ means – (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code; (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code; (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

<sup>2</sup> (U) Section 101(i) of FISA defines “United States person” as follows:

a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

3



4

~~TOP SECRET//SI//ORCON/NOFORN~~



~~TOP SECRET//SI//ORCON/NOFORN~~

certifications will either possess foreign intelligence information about the persons, groups, or entities covered by the certifications or are likely to receive or communicate foreign intelligence information concerning these persons, groups, or entities. This requirement is reinforced by the Attorney General's Acquisition Guidelines, which provide that an individual may not be targeted unless a significant purpose of the targeting is to acquire foreign intelligence information that the person possesses, is reasonably expected to receive, and/or is likely to communicate.

(U) Under NSA's FISC-approved targeting procedures, NSA targets a particular non-United States person reasonably believed to be located outside the United States by tasking facilities used by that person who possesses or who is likely to communicate or receive foreign intelligence information. A facility (also known as a "selector") is a specific communications identifier tasked to acquire foreign intelligence information that is to, from, or about a target. A "facility" could be a telephone number or an identifier related to a form of electronic communication, such as an e-mail address.<sup>5</sup> In order to acquire foreign intelligence information from or with the assistance of an electronic communications service provider, NSA first uses the identification of a facility to acquire the relevant communications. Then, after applying its targeting procedures (further discussed below) and other internal reviews and approvals, NSA "tasks" that facility in the relevant tasking system. The facilities are in turn provided to electronic communication service providers who have been served with the required directives under the certifications.

(U) After information is collected from those tasked facilities, it is subject to FISC-approved minimization procedures. NSA's minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is routed to NSA. However, NSA's minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA, FBI, and NCTC, in accordance with NSA's targeting and minimization procedures, must in turn be processed by CIA, FBI, and NCTC in accordance with their respective FISC-approved Section 702 minimization procedures.<sup>6</sup>

(U) NSA's targeting procedures address, among other subjects, the manner in which NSA will determine that a person targeted under Section 702 is a non-United States person reasonably believed to be located outside the United States, the post-targeting analysis conducted on the facilities, and the documentation required.

5

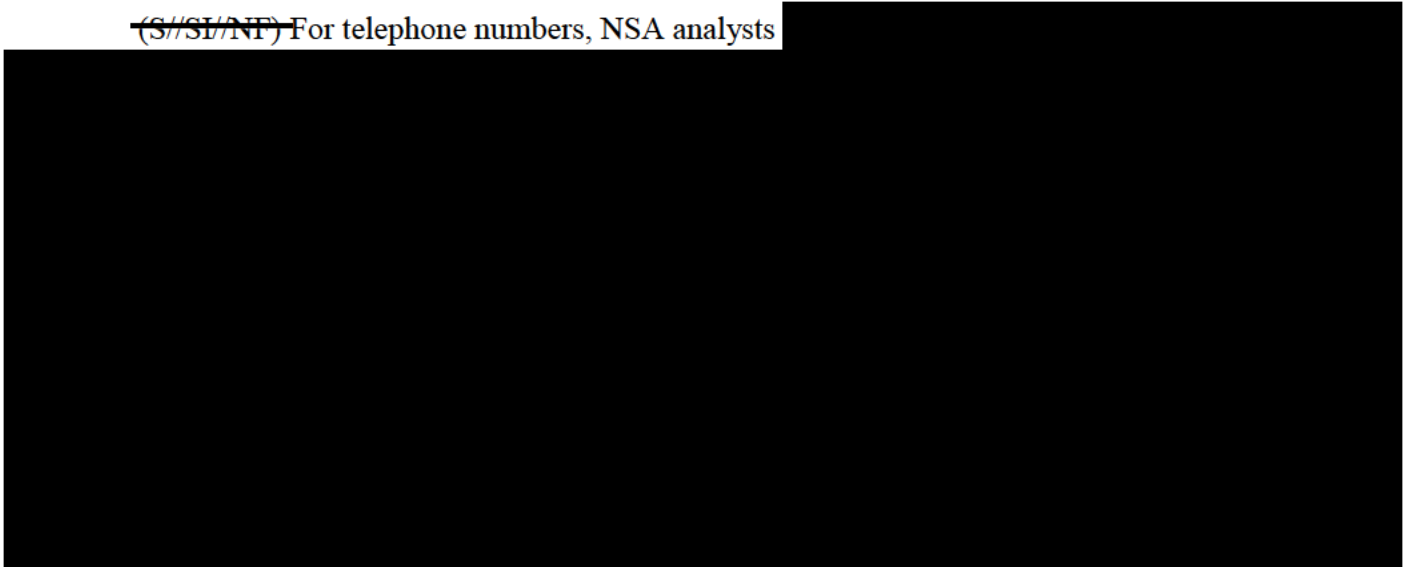
6

~~TOP SECRET//SI//ORCON/NOFORN~~

**(U) A. Pre-Tasking Location**

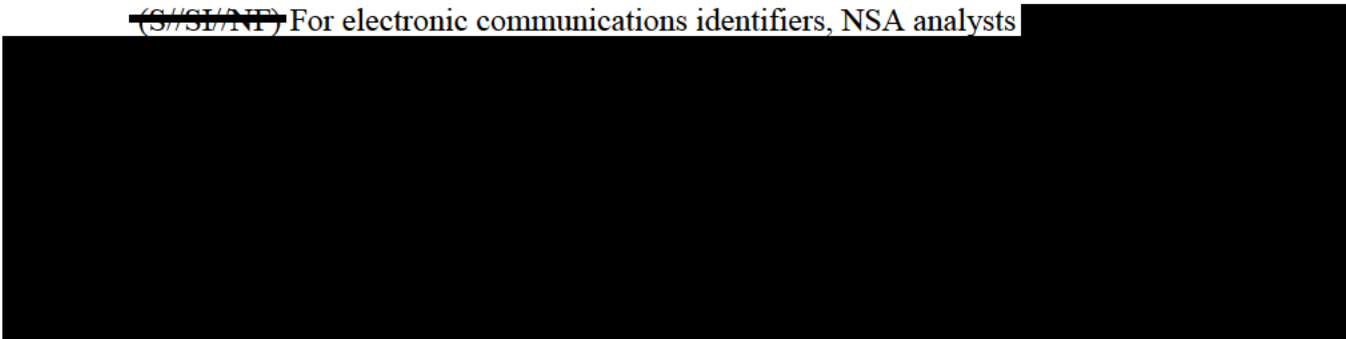
**(U) 1. Telephone Numbers**

~~(S//SI//NF)~~ For telephone numbers, NSA analysts



**(U) 2. Electronic Communications Identifiers**

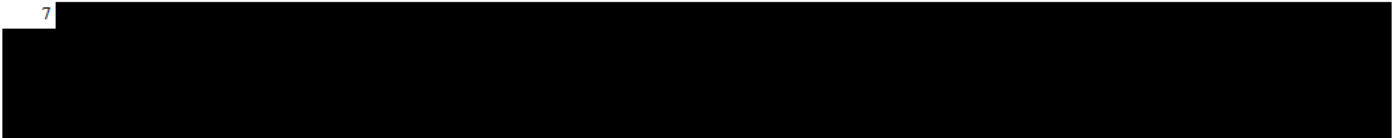
~~(S//SI//NF)~~ For electronic communications identifiers, NSA analysts



**(U) B. Pre-Tasking Determination of United States Person Status**

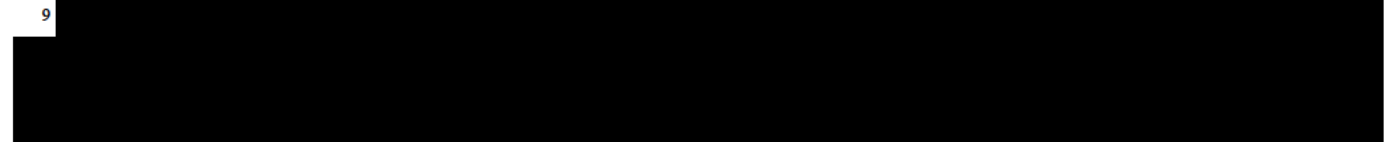


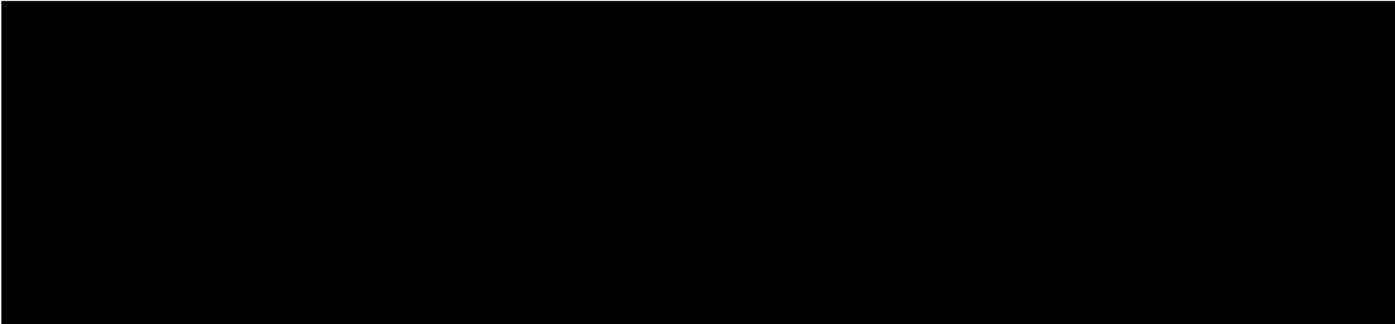
7



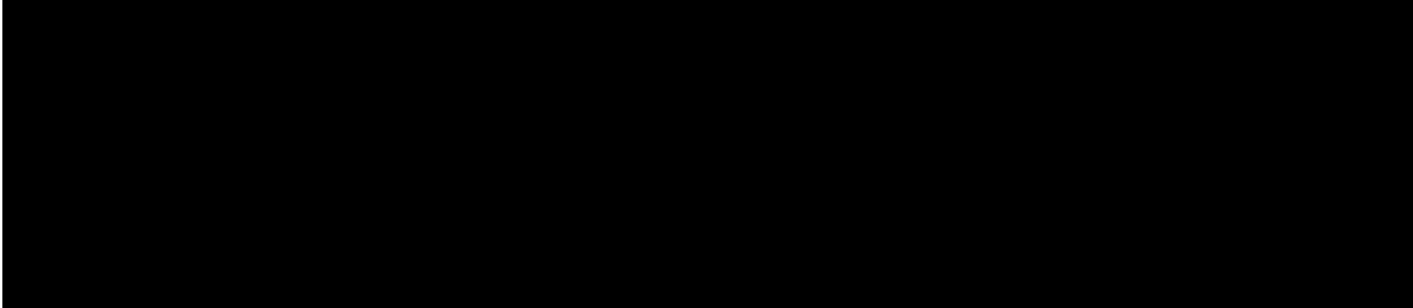
<sup>8</sup> (U) Analysts also check this system as part of the “post-targeting” analysis described below.


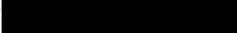


9




~~TOP SECRET//SI//ORCON//NOFORN~~

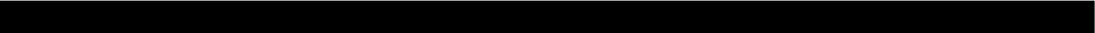
(U) **C. Post-Tasking Checks**



(S)  NSA also requires that tasking analysts review information collected from the facilities they have tasked. With respect to NSA's review of  <sup>11</sup> a notification e-mail is sent to the tasking team upon initial collection for the facility. NSA analysts are expected to review this collection within five business days to confirm that the user of the facility is the intended target, that the target remains appropriate to the certification cited, and that the target remains outside the United States. Analysts are then responsible to review traffic on an on-going basis to ensure that the facility remains appropriate under the authority. 

 Should traffic not be viewed at least once every 30 business days, a notice is sent to the tasking team and their management, who then have the responsibility to follow up.

(U) **D. Documentation**

~~(S//NF)~~ The procedures provide that analysts will document in the tasking database a citation to the information leading them to reasonably believe that a targeted person is located outside the United States. The citation is a reference that includes the source of the information,  enabling oversight personnel to locate and review the information that led the analyst to his/her reasonable

10



11

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

belief. Analysts must also identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information.

~~(S//NF)~~ NSA [REDACTED] an existing database tool, for use by its analysts for Section 702 tasking and documentation purposes. [REDACTED] to assist analysts as they conduct their work. This tool has been modified over time to accommodate the requirements of Section 702, to include, for example, certain fields and features for targeting, documentation, and oversight purposes. Accordingly, the tool allows analysts to document the required citation to NSA records on which NSA relied to form the reasonable belief that the target was located outside the United States. [REDACTED]

[REDACTED] The tool has fields for the certification under which the target falls, and for the foreign power as to which the analyst expects to collect foreign intelligence information. Analysts fill out various fields [REDACTED] each facility, as appropriate, including the citation to the information on which the analyst relied in making the foreignness determination.

(U) NSA's targeting procedures also require analysts to identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information and provide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning that foreign power or foreign territory.

(U) NSA also includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular facility was requested. The intent of the TAR is to memorialize why the analyst is requesting targeting, and provides a linkage between the user of the facility and the foreign intelligence purpose covered by the certification under which it is being tasked. The joint oversight team assesses that the TAR has improved the oversight team's ability to understand NSA's foreign intelligence purpose in tasking facilities.

~~(S//NF)~~ [REDACTED]

[REDACTED] Entries are reviewed before a tasking can be finalized. Records from this tool are maintained and compiled for oversight purposes. For each facility, a record can be compiled and printed showing certain relevant fields, such as: the facility, the certification, the citation to the record or records relied upon by the analyst, [REDACTED] the analyst's foreignness explanation, the targeting rationale, [REDACTED] These records, referred to as "tasking sheets," are reviewed by the Department of Justice's National Security Division (NSD), and also provided to the Office of the Director of National Intelligence (ODNI), as part of the oversight process.

~~(S//NF)~~ The source records cited on these tasking sheets are contained in a variety of NSA data repositories. These records are maintained by NSA and, when requested by the joint team, are produced to verify determinations recorded on the tasking sheets. Other source records may consist of "lead information" from other agencies, such as disseminated intelligence reports or lead information [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

### (U) F. Internal Procedures

(U) NSA has instituted internal training programs, access control procedures, standard operating procedures, compliance incident reporting measures, and similar processes to implement the requirements of the targeting procedures. Only analysts who have received certain types of training and authorizations are provided access to the Section 702 program data. These analysts must complete an NSA OGC and OCCO training program; review the targeting, minimization, and querying procedures as well as other documents filed with the certifications; and pass a competency test. The databases NSA analysts use are subject to audit and review by OCCO. For guidance, analysts consult standard operating procedures, supervisors, OCCO personnel, and NSA OGC attorneys.

(U) NSA's targeting and minimization procedures also require NSA to conduct oversight activities and make any necessary reports, including those relating to incidents of non-compliance, to NSA's Office of the Inspector General (OIG) and NSA OGC. NSA's OCCO reviews all Section 702 taskings and conducts spots checks of disseminations based in whole or in part on Section 702-acquired information. The Directorate of Operations Information and Intelligence Analysis organization also maintains and updates an NSA internal website regarding the implementation of, and compliance with, the Section 702 authorities.

(U) NSA has established standard operating procedures for incident tracking and reporting to NSD and ODNI. Compliance officers work with NSA analysts and CIA and FBI points of contact, as necessary, to compile incident reports that are forwarded to both NSA OGC and OIG. NSA OGC forwards the incidents to NSD and ODNI.

(U) On a more programmatic level, under the guidance and direction of the Compliance Group, NSA has implemented and maintains a Comprehensive Mission Compliance Program (CMCP) designed to effect verifiable conformance with the laws and policies that afford privacy protections during NSA missions. The Compliance Group complements and reinforces the intelligence oversight program of NSA's OIG and oversight responsibilities of NSA OGC.

(U) A key component of the CMCP is an effort to manage, organize, and maintain the authorities, policies, and compliance requirements that govern NSA mission activities. This effort,

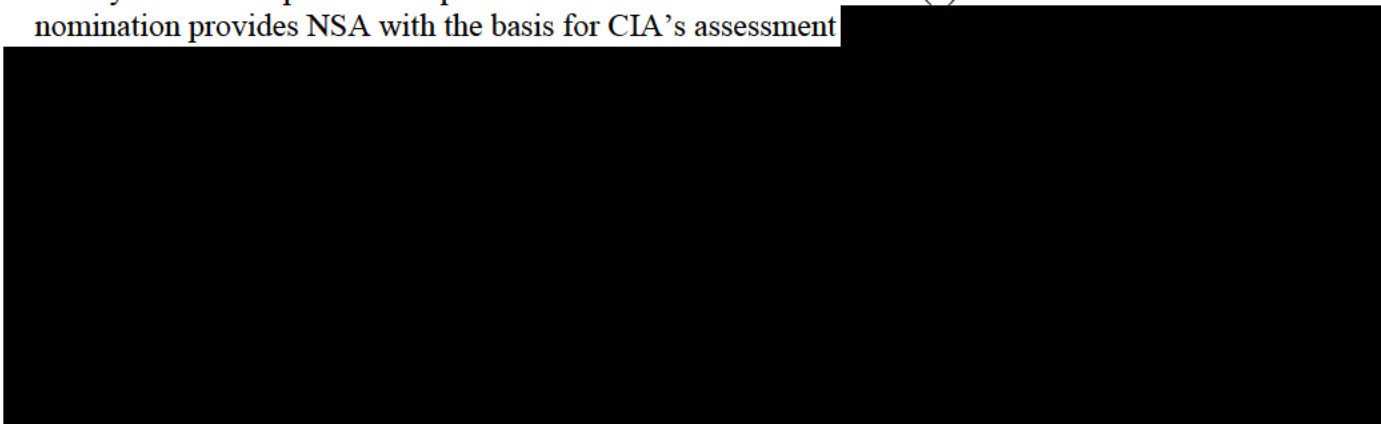
~~TOP SECRET//SI//ORCON//NOFORN~~

known as “Rules Management,” focuses on two key components: (1) the processes necessary to better govern, maintain, and understand the authorities granted to NSA; and (2) technological solutions to support (and simplify) Rules Management activities. The Authorities Integration Group coordinates NSA’s use of the Verification of Accuracy process originally developed for other FISA programs to provide an increased level of confidence that factual representations to the FISC or other external decision makers are accurate and based on an ongoing, shared understanding among operational, technical, legal, policy, and compliance officials within NSA. NSA has also developed a Verification of Interpretation review to help ensure that NSA and its external overseers have a shared understanding of key terms in Court orders, minimization procedures, and other documents that govern NSA’s FISA activities. The Compliance Group conducts the Mission Compliance Risk Assessment (MCRA) that assesses the risk of non-compliance with the rules designed to protect privacy and to safeguard information. Risks are assessed annually by authority and/or function for SIGINT and Cybersecurity Missions. The results are used to inform management decisions, priorities, and resource allocations regarding the NSA/CSS Comprehensive Mission Compliance Program (CMCP).

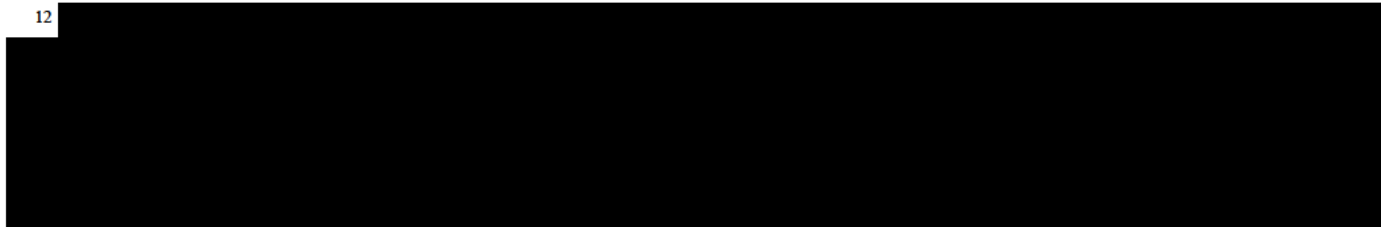
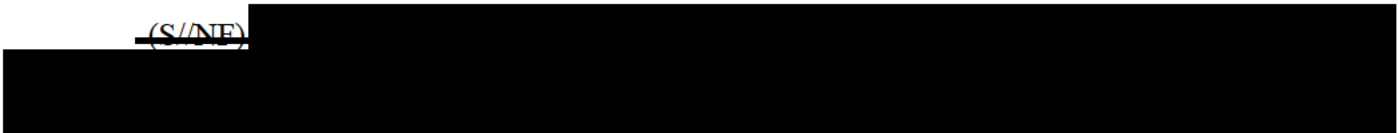
(U) **II. Overview – CIA**

(U) **A. CIA’s Role in Targeting**

~~(S//NF)~~ Although CIA does not target or acquire communications pursuant to Section 702, CIA has put in place a process, in consultation with NSA, FBI, NSD, and ODNI, to identify foreign intelligence targets to NSA. Based on its foreign intelligence analysis, CIA may “nominate” a facility to NSA for potential acquisition under one of the Section 702(h) certifications. The nomination provides NSA with the basis for CIA’s assessment



~~(S//NF)~~



~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED] Nominations are reviewed and approved by a targeting officer's first line manager, a component legal officer, a senior operational manager, and the FISA Program Office prior to export to NSA.<sup>13</sup> [REDACTED]

~~(S//NF)~~ The FISA Program Office was established in December 2010 [REDACTED]

[REDACTED] and is charged with providing strategic direction for the management and oversight of CIA's FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA, and FBI. In addition, the office leads the day-to-day FISA compliance efforts [REDACTED]. The primary responsibilities of the FISA Program Office are to provide strategic direction for data handling and management of FISA/702 data, as well as to ensure that all Section 702 collection is properly tasked and that CIA is complying with all compliance and purge requirements.

#### (U) B. Oversight and Compliance

(U) CIA's FISA compliance program is managed by its FISA Program Office in coordination with CIA OGC. CIA provides small group training to personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Access to unminimized Section 702-acquired communications is limited to trained personnel. CIA attorneys embedded with operational elements that have access to unminimized Section 702-acquired information also respond to inquiries regarding nomination, minimization, and querying questions. Identified incidents of noncompliance with CIA's minimization and querying procedures are generally reported to NSD and ODNI by CIA OGC.

(U)<sup>13</sup> ~~(S//NF)~~ This nomination approval process was the one in place during the reporting period. However, on 21 October 2021, CIA's nominations process was revised to require approval by only the targeting officer's first line manager and the FISA Program Office. Throughout the process, both component legal officers and CIA's FISA attorneys are available for consultation regarding whether the nomination is in compliance with Section 702 of FISA and NSA's targeting procedures. The Government assesses this change eliminates redundancy in CIA's nomination process.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~**(U) III. Overview – NCTC****(U) A. NCTC’s Handling of Section 702 data**

~~(S//NF)~~ NCTC does not target or acquire communications pursuant to Section 702. In addition, NCTC does not currently have a process in place to identify or nominate foreign intelligence targets to NSA. However, like CIA and FBI, NCTC may request to be [REDACTED] on unminimized data (pertaining to counterterrorism) from Section 702 facilities already tasked by NSA. NCTC applies its Section 702 minimization and querying procedures to Section 702 [REDACTED] data.

~~(S//NF)~~ NCTC, in consultation with NSD, developed an electronic and data storage system, known as [REDACTED] to retain and process unminimized FBI-collected FISA-acquired information in accordance with NCTC’s Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of FISA. In consultation with NSD, ODNI, NSA, and FBI, NCTC modified [REDACTED] to (i) provide additional compliance capabilities in support of [REDACTED] FISA Section 702-acquired counterterrorism data and (ii) monitor compliance with NCTC’s minimization and querying procedures for Section 702-acquired counterterrorism data. In addition to documenting compliance with the Section 702 minimization and querying procedures requirements, [REDACTED] also documents the requests for [REDACTED] of Section 702-acquired information. This documentation includes the foreign intelligence justification (pertaining to counterterrorism) for [REDACTED] the facility and supervisory concurrence with an analyst’s request.

~~(S//NF)~~ [REDACTED] communications from Section 702 tasked facilities are stored within [REDACTED] where only properly trained and authorized analysts are able to query them. As a supplement to the requirements of NCTC’s minimization and querying procedures, NCTC’s internal business process requires that NCTC analysts provide a written justification for each query, as well as a written justification for each minimization action to mark a product as meeting the retention standard in order to document how the query or minimization was compliant with the standards in NCTC’s minimization or querying procedures, as applicable. By internal policy, all [REDACTED] requests and minimization actions must be reviewed and approved [REDACTED] by the analyst’s supervisor.

(U) ~~(S//NF)~~ NCTC personnel may disseminate Section 702-acquired information of or concerning an unconsenting United States person if that information meets the standard for dissemination pursuant to Section D of NCTC’s minimization procedures.

~~(S//NF)~~ [REDACTED] NCTC’s Compliance and Transparency Group (hereinafter, “NCTC Compliance”) within the Office of Data Strategy and Compliance (ODSC) conducts periodic reviews of Section 702 query logs and minimization logs, as well as NCTC Section 702 disseminations in order to verify compliance with NCTC’s minimization procedures and identify the need for system modifications, enhancements, or improvements to training materials or analyst work aids.

~~TOP SECRET//SI//ORCON/NOFORN~~



~~TOP SECRET//SI//ORCON//NOFORN~~~~(S//NF)~~

Pursuant to Section A.6 of NCTC's minimization procedures,

#### **(U) B. Oversight and Compliance**

(U) NCTC's FISA compliance program is managed by NCTC Compliance in coordination with NCTC Legal. NCTC provides training to all NCTC personnel who may access unminimized FISA-acquired information. Access to unminimized Section 702-acquired communications is limited to trained personnel. NCTC compliance personnel and attorneys also respond to inquiries regarding minimization and querying questions. Identified incidents of noncompliance with NCTC's minimization procedures and querying procedures are reported to NSD and ODNI generally by NCTC Compliance or NCTC Legal personnel.

~~(S//NF)~~ NCTC Compliance was established in the fall of 2014 and is charged with providing strategic direction for the management and oversight of NCTC's access to and use of all datasets pursuant to executive order, statute, interagency agreement, applicable IC policy, and internal policy. This includes management and oversight of NCTC's FISA programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA, FBI, and CIA. In addition, the office leads the day-to-day FISA compliance efforts within NCTC. NCTC Compliance is responsible for providing strategic direction and internal oversight for data handling and management of Section 702 data, as well as administering and implementing NCTC Section 702 training, ensuring that all NCTC Section 702 collection is properly [REDACTED] minimized and disseminated, and that NCTC is complying with all minimization and querying procedures requirements.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~**(U) IV. Overview – FBI****(U) A. FBI's Role in Targeting – Nomination for Acquiring In-Transit Communications**

~~(S//NF)~~ Like CIA, FBI has developed a formal nomination process to identify foreign intelligence targets to NSA for the acquisition of [REDACTED] communications. [REDACTED]

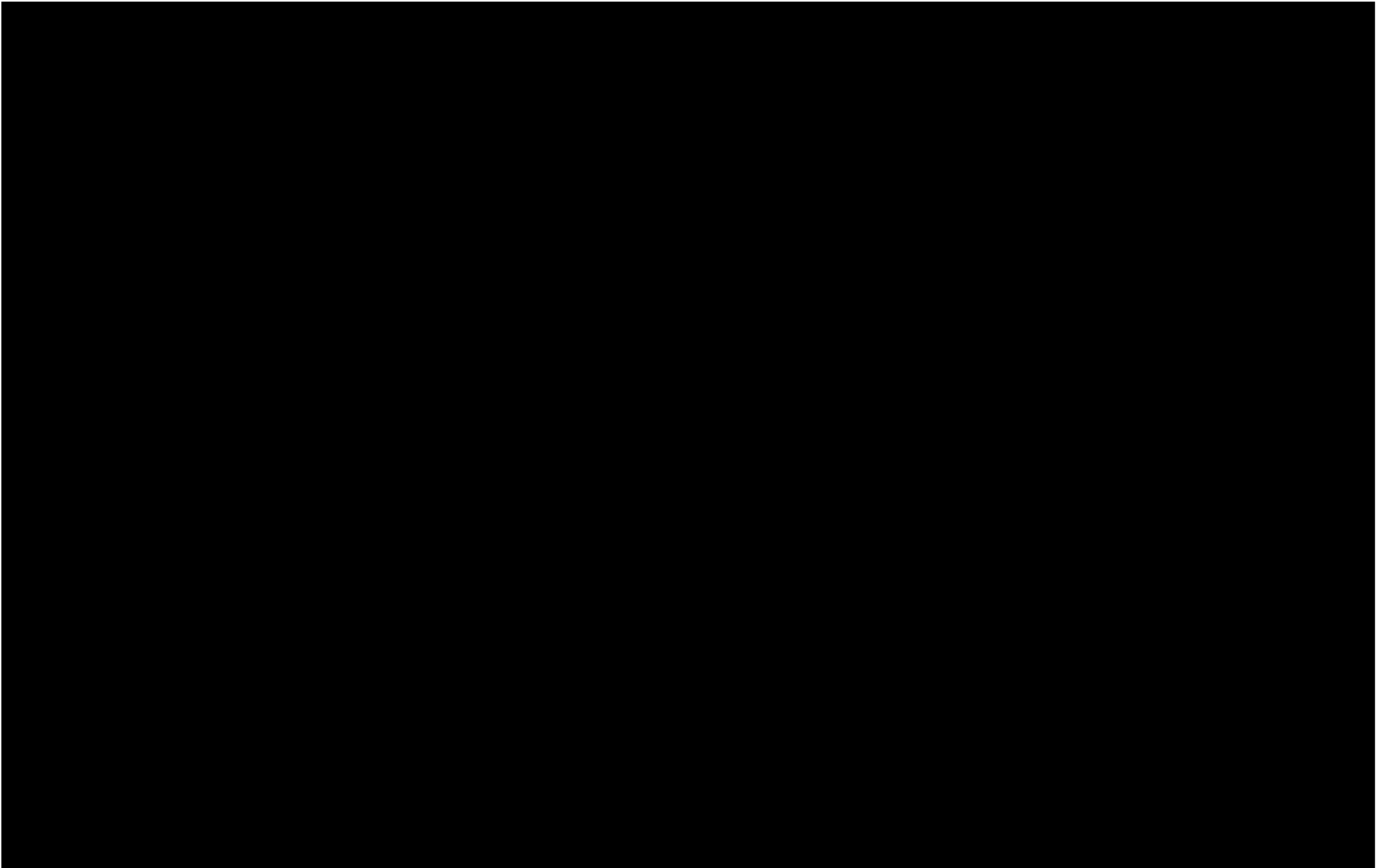
[REDACTED] including information underlying the basis for the foreignness determination and the foreign intelligence interest. FBI nominations are reviewed by FBI operational and legal personnel prior to export [REDACTED]

~~(S//NF)~~

[REDACTED] FBI targeting procedures require that NSA first apply its own targeting procedures to determine that the user of the Designated Account is a person reasonably believed to be outside the United States and is not a United States person. NSA is also responsible for determining that a significant purpose of the acquisition it requests is to obtain foreign intelligence information. After NSA designates accounts as being appropriate for [REDACTED] FBI must then apply its own, additional procedures, which require FBI to review NSA's conclusion of foreignness [REDACTED]

~~(S//NF)~~ More specifically, after FBI obtains the tasking sheet from NSA, it reviews the information provided by NSA regarding the location of the person and the non-United States person status of the person. [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

~~(S//NF)~~ Unless FBI locates information indicating that the user is a United States person or is located inside the United States [REDACTED]

~~(S//NF)~~ If FBI identifies information indicating that NSA's determination that the target is a non-United States person reasonably believed to be outside the United States may be incorrect, FBI provides this information to NSA and does not approve [REDACTED]

**(U) C. Documentation**

~~(S//NF)~~ The targeting procedures require that FBI retain the information [REDACTED] in accordance with its records retention policies [REDACTED]. FBI uses a multi-page checklist for each Designated Account to record the results of its targeting process, as laid out in its standard operating procedures, commencing with [REDACTED] extending through [REDACTED].

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

██████████ and culminating in approval or disapproval of the acquisition. In addition, FBI's standard operating procedures call for ██████████ ██████████ depending on the circumstances, which are maintained by FBI with the applicable checklist. FBI also retains with each checklist any relevant communications ██████████ regarding its review ██████████ information. Additional checklists have been created to capture information on requests withdrawn by ██████████ or not approved by FBI.

#### (U) **D. Implementation, Oversight, and Compliance**

~~(S//NF)~~ FBI's implementation and compliance activities are overseen by FBI OGC, particularly the National Security and Cyber Law Branch (NSCLB), as well as FBI's Technology and Data Innovation Section (TDI), FBI's ██████████ and FBI's Inspection Division (INSD). ██████████

██████████ TDI has the lead responsibility in FBI for ██████████ requests ██████████ TDI personnel are trained on FBI's targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests ██████████ ██████████ TDI also has the lead responsibility for facilitating FBI's nominations to NSA ██████████ TDI, NSCLB, NSD, and ODNI have all worked on training FBI personnel to ensure that FBI nominations and post-tasking review comply with NSA's targeting procedures. With respect to minimization, FBI has created a mandatory online training that all FBI agents and analysts must complete prior to gaining access to unminimized Section 702-acquired data in FBI ██████████

██████████ In addition, NSD conducts training on the Section 702 minimization procedures at multiple FBI field offices each year.<sup>14</sup>

(U) ~~(S//NF)~~ FBI's targeting procedures require periodic reviews by NSD and ODNI at least once every 60 days. FBI must also report incidents of non-compliance with FBI targeting procedures to NSD and ODNI within five business days of learning of the incident. TDI and NSCLB are the lead FBI elements in ensuring that NSD and ODNI received all appropriate information with regard to these two requirements.

#### (U) **V. Overview – Minimization and Querying**

(U) After a facility has been tasked for collection, non-publicly available information collected as a result of these taskings that concerns United States persons must be minimized; if the Government queries that collection, it must follow specific query rules. The FISC-approved minimization procedures require such minimization in the acquisition, retention, and dissemination of foreign intelligence information. The FISC-approved querying procedures set rules for using United States person and non-United States person identifiers to query unminimized Section 702-acquired information. Prior to the FISA Amendments Reauthorization Act of 2017 codification, the

---

<sup>14</sup> (U) As noted above, onsite field office reviews were suspended in March 2020. NSD resumed field office reviews remotely in February 2021. Thus, NSD only conducted onsite training at field offices for a portion of this reporting period.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

minimization procedures contained querying rules. The 2018 certifications were the first certifications to contain the newly required querying procedures.

(U) As a general matter, minimization procedures under Section 702 are similar in most respects to minimization under other FISA orders. For example, the Section 702 minimization procedures, like those under certain other FISA court orders, allow for sharing of certain unminimized Section 702 information among NSA, FBI, CIA and NCTC. Similarly, the procedures for each agency require special handling of intercepted communications that are between attorneys and clients, as well as foreign intelligence information concerning United States persons that is disseminated to foreign governments.

(U) Section 702 minimization procedures do, however, impose additional obligations or restrictions as compared with the minimization procedures associated with authorities granted under Titles I and III of FISA. For example, the Section 702 minimization procedures require, with limited exceptions, the purge of any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States, but is in fact located inside the United States at the time the communication is acquired, or was in fact a United States person at the time of targeting.

(U) NSA, CIA, NCTC, and FBI have created systems to track the purging of information from their systems. CIA, NCTC, and FBI receive incident notifications from NSA to document when NSA has identified Section 702 information that NSA is required to purge according to its procedures, so that CIA and FBI can meet their respective obligations.

(U) With passage of the FISA Amendments Reauthorization Act of 2017, Congress amended Section 702 to require that querying procedures be adopted by the Attorney General, in consultation with the DNI. Section 702(f)(1) requires that the querying procedures be consistent with the Fourth Amendment and that they include a technical procedure whereby a record is kept of each United States person term used for a query. Congress added other requirements in Section 702(f), which pertain to accessing certain results of queries conducted by FBI. Specifically, under Section 702(f)(2)(A), an order from the FISC is now required before FBI can review the contents of a query using a United States person query term when the query was not designed to find and extract foreign intelligence information and was performed in connection with a predicated criminal investigation that does not relate to national security.

(U) Queries may be conducted in two types of unminimized Section 702-acquired information: (i) Section 702-acquired *content* and (ii) Section 702-acquired *metadata*. Query terms may be date-bound, and may include alphanumeric strings, such as telephone numbers, email addresses, or terms, such as a name, that can be used individually or in combination with one another. Pursuant to FISC-approved procedures, an agency can only query Section 702 information if the query is reasonably likely to retrieve foreign intelligence information or, in the case of FBI, evidence of a crime. This standard applies to all Section 702 queries, regardless of whether the term concerns a United States person or non-United States person.

(U) The agencies have similar querying procedures. For example, the agencies' procedures require a written statement of facts justifying that the use of any such identifier as a query selection

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

term of Section 702-acquired content is reasonably likely to retrieve foreign intelligence information or, in the instance of FBI, evidence of a crime. Some querying rules are unique to individual agencies. For example, NSA's Section 702 querying procedures also require that any United States person query term used to identify and select unminimized section 702-acquired content must first be approved by NSA's Office of General Counsel and that such an approval include a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to retrieve foreign intelligence information. In addition, with respect to queries of Section 702-acquired metadata using a United States person identifier, NSA's querying procedures require that NSA analysts document the basis for each metadata query prior to conducting the query.

~~TOP SECRET//SI//ORCON//NOFORN~~

Congress of the United States  
House of Representatives  
Washington, DC 20515-0305

February 15, 2023

Christopher Wray  
Director  
Federal Bureau of Investigation  
935 Pennsylvania Avenue, NW  
Washington, D.C. 20535

Dear Director Wray,

In December 2022, Department of Justice and the Office of the Director of National Intelligence declassified a 2021 report<sup>1</sup> detailing continued abuses of Section 702 of the Foreign Intelligence Surveillance Act (FISA). Specifically, the report mentions one instance in which “FBI queried the names of a local political party” and one instance in which “an [intelligence analyst] conducted approximately [redacted] queries...using only the name of a U.S. congressman.” These instances should frighten every American and Congress deserves an explanation for them.

FISA Section 702 was designed to grant federal intelligence agencies the authorities to monitor non-U.S. persons located outside the United States to acquire foreign intelligence information. However, over the years Section 702 has led to the abundant collection of information related to Americans and information that is not foreign intelligence. While concerning, matters are made worse by continuous reports that federal agents are querying the 702 database specifically looking for information related to Americans. These “backdoor searches” are a violation of the Fourth Amendment and cannot continue.

During the last reauthorization of Section 702, Congress considered an amendment to require a warrant for access to 702 data relating to U.S. persons. However, federal intelligence agencies used scare tactics to convince legislators that unchecked use of this information is the only way to keep our nation safe from harm. The Fourth Amendment to the U.S. Constitution is clear—Americans have the right to be free from warrantless surveillance by government bureaucrats.

As Congress begins conversations on whether FISA 702 authorities should be reauthorized beyond December 31, 2023, please answer the following questions by March 3, 2023:

1. Was the “U.S. congressman” mentioned in footnote 92 made aware of the search of their name in the 702 database? If not, please explain the reasoning.

---

<sup>1</sup> *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence* (Dec. 2021), <https://www.intelligence.gov/assets/documents/702%20Documents/declassified/24th-Joint-Assessment-of-FISA-702-Compliance.pdf>.

2. What steps were taken to discipline the intelligence analyst responsible for the query conducted in footnote 92?
3. Similarly, what steps were taken to discipline the FBI agent mentioned on page 58 who “queried the names of a local political party”?
4. For the below three groups, over the last five years, how many times were each queried? How many times did those queries return hits? How many times were those hits opened for review?
  - a. Members of Congress or congressional staff;
  - b. Political party officials;
  - c. Campaign personnel and candidates.
5. What steps have been taken to remind analysts and other personnel with access to the database that the two searches mentioned above are not permitted under law? If none, please explain why. Please provide a copy of the latest comprehensive guidance disseminated to agents.
6. What new steps have been taken to minimize non-foreign intelligence information and information that relates to Americans in the database to remove the temptation for agents to inappropriately query for such information?

If the responses to any of the questions above require a classified setting, please contact my office so that a briefing may be promptly arranged.

Sincerely,



Andy Biggs  
Member of Congress



UNCLASSIFIED



February 28, 2023



The Honorable Charles E. Schumer  
Majority Leader  
United States Senate  
Washington, DC 20510

The Honorable Mitch McConnell  
Minority Leader  
United States Senate  
Washington, DC 20510

The Honorable Kevin McCarthy  
Speaker  
U.S. House of Representatives  
Washington, DC 20515

The Honorable Hakeem S. Jeffries  
Minority Leader  
U.S. House of Representatives  
Washington, DC 20515

Dear Leader Schumer, Leader McConnell, Speaker McCarthy, and Leader Jeffries:

As the 118<sup>th</sup> Congress begins, we urge you to promptly reauthorize a key foreign intelligence authority—Title VII of the Foreign Intelligence Surveillance Act (FISA)—before it expires on December 31, 2023.

Title VII of FISA, and in particular Section 702, has been a critical authority for the Intelligence Community (IC) and Department of Justice (DOJ) since its passage in 2008. The authority allows the U.S. Government to acquire foreign intelligence information from individual terrorists, weapons proliferators, hackers, and other foreign intelligence targets located overseas who operate using U.S. electronic communications service providers. It also requires the IC and DOJ to comply with robust privacy and civil liberties safeguards, which are overseen by all three branches of government. As the examples below demonstrate, the information acquired using Section 702 plays a key role in keeping the United States, its citizens, and its allies safe and secure.

Given this, the reauthorization of Title VII is a top legislative priority for this Administration. Both the IC and DOJ thus stand ready to provide you and your offices with information about how Section 702 is used to produce unique and timely intelligence, and the steps we have taken to strengthen compliance with FISA's privacy and civil liberties safeguards. As in past reauthorization cycles, the IC and DOJ are committed to engaging with Congress on potential improvements to the authority that fully preserve its efficacy.

\* \* \* \* \*

UNCLASSIFIED

The Honorable Charles E. Schumer  
The Honorable Mitch McConnell  
The Honorable Kevin McCarthy  
The Honorable Hakeem S. Jeffries

Over the last 15 years, Section 702 has proven invaluable again and again in protecting American lives and U.S. national security:

Section 702 has been used to identify and protect against national security threats to the United States and its allies, to include both conventional and cyber threats posed by the People's Republic of China, Russia, Iran, and the Democratic People's Republic of Korea.

- Section 702-acquired information has been used to identify multiple foreign ransomware attacks on U.S. critical infrastructure. This intelligence positioned the U.S. Government to respond to and mitigate these events, and in some instances prevent significant attacks on U.S. networks.
- Section 702-acquired information related to sanctioned foreign adversaries was used in U.S. Government efforts to stop components for weapons of mass destruction from reaching foreign actors.
- Section 702 has identified threats to U.S. troops and disrupted planned terrorist attacks both at home and abroad, and contributed to the United States' successful operation against Ayman al-Zawahiri in 2022.
- Section 702 has resulted in the identification and disruption of hostile foreign actors' attempts to recruit spies in the United States or send their operatives to the United States.
- Section 702 information has identified key economic security risks, including strategic malign investment by foreign actors in certain U.S. companies.

It has also become clear that there is no way to replicate Section 702's speed, reliability, specificity, and insight.

\* \* \* \* \*

The comprehensive system Congress designed to ensure this irreplaceable intelligence tool protects the privacy and civil liberties of U.S. persons has worked. When incidents of non-compliance have been identified, remedial steps have been taken to ensure the authority is being implemented consistent with its limited scope.

Because Section 702 can only be used to target individual *non-U.S. persons located outside the United States*, it may not be directed against Americans at home or abroad, or any person, regardless of nationality, known to be located in the United States. It also cannot be used to collect against a foreign person overseas if the intended purpose is to target someone located in the United States. Each target must meet specific foreign intelligence criteria and any information can only be collected, analyzed, and disseminated according to detailed court-approved procedures. It cannot

The Honorable Charles E. Schumer  
The Honorable Mitch McConnell  
The Honorable Kevin McCarthy  
The Honorable Hakeem S. Jeffries

be used to gather data in bulk. Every court to consider the Section 702 program has found it to be constitutional.

Compliance with these strictures is subject to a comprehensive oversight regime involving all three branches of our Government. First, the Foreign Intelligence Surveillance Court (FISC)—an Article III court—conducts a comprehensive review of the program annually, evaluating certifications submitted by the Attorney General and the Director of National Intelligence that identify appropriate categories of foreign intelligence information as well as accompanying targeting, acquisition, and minimization procedures. Additionally, the FISC has sought the views of outside experts (*Amicus Curiae*) on multiple occasions as it exercises its rigorous and ongoing oversight of the U.S. Government’s implementation of and compliance with these procedures. Second, DOJ and the Office of the Director of National Intelligence scrutinize all Section 702 collection decisions, review U.S. person queries, and evaluate and take remedial action to address identified incidents of non-compliance. Finally, the congressional intelligence and judiciary committees receive semi-annual compliance reporting and regular briefings to facilitate their stringent oversight.

In addition to the privacy protections contained in Section 702, separate provisions in Title VII of FISA provide heightened standards for other foreign intelligence activities conducted overseas. For example, Title VII requires an individual court order before the U.S. Government can conduct surveillance against an American located overseas when the Government has established it has probable cause to believe the target is “a foreign power, an agent of a foreign power, or an officer or employee of a foreign power.” Other provisions of Title VII support congressional oversight by requiring the release of detailed information about how the U.S. Government uses the authority.

\* \* \* \* \*

As noted at the outset, we stand ready to help you and your offices get the information you need as you consider the reauthorization of Title VII before December 31, 2023. To that end, our staff will be offering briefings on Section 702, including at the classified level, on the specific operational successes enabled by Section 702, and the actions we have taken to implement Section 702’s privacy and civil liberties’ protections. We also encourage you to contact Matt Rhoades, Assistant Director of National Intelligence for Legislative Affairs, or Carlos Uriarte, Assistant Attorney General for Legislative Affairs, if you would like any further information or have any questions.

UNCLASSIFIED

The Honorable Charles E. Schumer  
The Honorable Mitch McConnell  
The Honorable Kevin McCarthy  
The Honorable Hakeem S. Jeffries

We look forward to working with you over the coming year to reauthorize this fundamentally critical national security tool.



---

Merrick B. Garland  
Attorney General



---

Avril D. Haines  
Director of National Intelligence

UNCLASSIFIED

The Honorable Charles E. Schumer  
The Honorable Mitch McConnell  
The Honorable Kevin McCarthy  
The Honorable Hakeem S. Jeffries

Cc:

The Honorable Kamala Harris, President, U.S. Senate  
The Honorable Patty Murray, President Pro Tempore, U.S. Senate  
The Honorable Richard J. Durbin, Chair, Committee on the Judiciary, U.S. Senate  
The Honorable Lindsey O. Graham, Ranking Member, Committee on the Judiciary, U.S. Senate  
The Honorable Jim Jordan, Chairman, Committee on the Judiciary, U.S. House of Representatives  
The Honorable Jerrold L. Nadler, Ranking Member, Committee on the Judiciary, U.S. House of  
Representatives  
The Honorable Mark R. Warner, Chairman, Select Committee on Intelligence, U.S. Senate  
The Honorable Marco Rubio, Vice Chairman, Select Committee on Intelligence, U.S. Senate  
The Honorable Michael Turner, Chairman, Permanent Select Committee on Intelligence, U.S.  
House of Representatives  
The Honorable Jim Himes, Ranking Member, Permanent Select Committee on Intelligence, U.S.  
House of Representatives

## SCOTUS appears skeptical of Biden's student debt relief plan

A majority of justices appeared dubious about the Biden administration's pandemic-related legal justification for the sweeping debt relief program.

PAGE 3



## Always Trump?

His hold on a portion of voters is having a deep impact on the race.

PAGE 5

## PACs poised to supercharge California Senate campaign

A wide-open field of Democrats could unleash millions in outside spending.

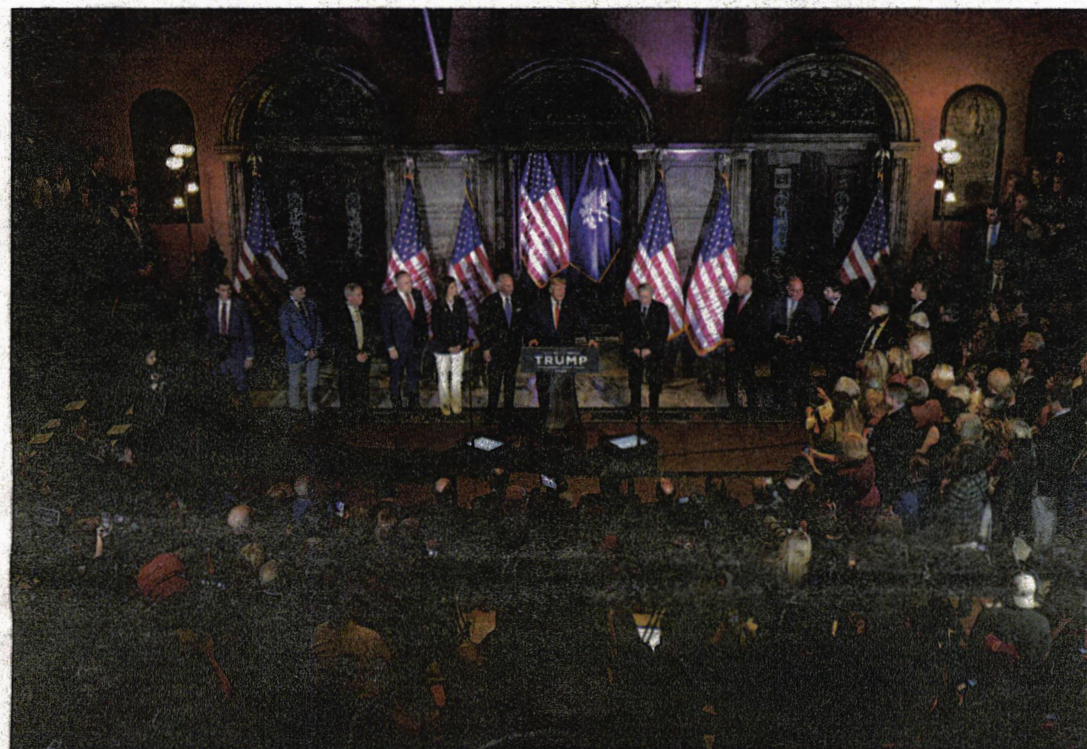
PAGE 6



## Matt Wuerker

The cartoonist's daily take on the world of politics.

PAGE 18



ALEX BRANDON/AP

Donald Trump's attacks on potential GOP primary opponents, and his warning to party leaders to stay away from the entitlement programs in their push to cut spending, are cleaving Republicans at every level.

## Trump ties GOP in knots over Medicare and Social Security

The former president is assailing his primary opponents for entertaining entitlement cuts in the past — and exacerbating divisions among Hill Republicans in the process

BY BURGESS EVERETT AND CAITLIN EMMA

Donald Trump is driving a wedge through the GOP over one of American politics' thorniest issues: the future of Medicare and Social Security.

The former president's attacks on potential GOP primary opponents, and his warning to party leaders to stay away from the popular entitlement programs in their push to cut spending, are cleaving Republicans at every level.

Lawmakers who once backed entitlement overhauls are now openly at odds with colleagues who'd prefer to soften their positions before they face voters in 2024. And a GOP pres-

ENTITLEMENTS on Page 13

## House GOP moving to let Jan. 6 defendants access Capitol footage

BY KYLE CHENEY, OLIVIA BEAVERS AND SARAH FERRIS

House Republicans are moving to provide defendants in Jan. 6-related cases access to thousands of hours of internal Capitol security footage, a move that could influence many of the ongoing prosecu-

tions stemming from 2021's violent attack.

Rep. Barry Loudermilk (R-Ga.), who chairs the House Administration Committee's oversight sub-panel, said the access for accused rioters and others — which Speaker Kevin McCarthy has greenlighted — would be granted on a "case-by-

case basis."

"Everyone accused of a crime in this country deserves due process, which includes access to evidence which may be used to prove their guilt or innocence," Loudermilk told POLITICO in a statement. "It is our intention to make available

REPUBLICANS on Page 10

## Republicans sink hope for easy surveillance reauthorization

House Republicans are preparing their own reform proposals for the controversial program

BY JORDAIN CARNEY

Congress and the Biden administration have started down a collision course as a controversial surveillance program is set to sunset this year, with lawmakers immediately indicating they would not accept the executive branch's opening offer.

The Justice Department and the intelligence community formally launched its reauthorization effort on Tuesday by floating to congressional leadership that the surveillance authority, known as Section 702, should be extended largely as is. Lawmakers all too happily shot down that trial balloon, previewing what will be a monthslong fight that could run right up to the Dec. 31 deadline with no clear path to

compromise.

There's no shortage of potential pitfalls. The administration won't just have to contend with usual antagonists in congressional Republicans, but also fellow Democrats who worry that the program doesn't have sufficient guardrails. The authority is designed to gather electronic communications of foreigners abroad, but also has the potential to sweep up the communications of Americans.

To add to the political headache, the Justice Department will need to win over a Republican House, where many of the lawmakers with oversight of the program are the same leading a sweeping investigation into alleged political moti-

SURVEILLANCE on Page 11

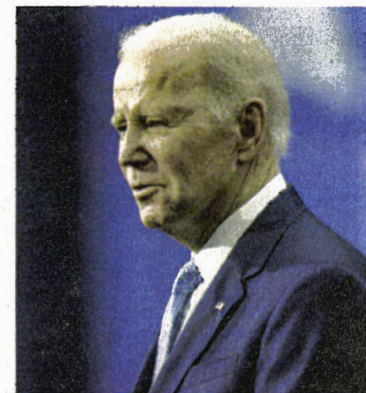
## Biden's deficit hawk persona has progressives feeling some bad deja vu

BY ADAM CANCRYN

Joe Biden spent the past two years pursuing and enacting massive domestic programs meant to remake the U.S. economy. But as he prepares a run for reelection, Biden is trying out a new economic persona: deficit hawk.

The president has made a fresh effort to sell his administration as a model of fiscal restraint in recent weeks, casting falling deficits as an increasingly central focus of his agenda. Biden now routinely touts a \$1.7 trillion drop in the deficit on his watch as a top accomplishment. When the president releases his new proposed budget next week,

BIDEN on Page 12



ANNA MONEYMAKER/GETTY IMAGES

President Joe Biden now routinely touts a \$1.7 trillion drop in the deficit as a top accomplishment.

# DOJ faces bipartisan (phalanx) of skeptics on FISA 702

**SURVEILLANCE** from Page 1

ations within the DOJ and the FBI. The party's relationship with the law enforcement apparatus soured sharply during former President Donald Trump's tenure, amid GOP accusations that the feds improperly targeted Trump and his allies.

A group of House Republicans are already discussing letting the surveillance authority sunset entirely, according to a GOP aide. And in a significant red flag for supporters of the currently written program, Rep. Jim Jordan (R-Ohio) — who chairs the House Judiciary Committee, one of the four congressional panels that will lead the Section 702 discussions — said he won't support extending the program without changes.

In fact, he isn't yet convinced that it needs to be continued at all.

"We're working on the kind of reforms we think need to happen, but frankly I think you should have to go get a warrant," Jordan said in a brief interview.

The Ohio Republican didn't support reauthorizing the program in January 2018, so his skepticism is hardly surprising. But his influence has grown significantly since then: He is now wielding a gavel and has transitioned from leadership foe to ally. And his panel is now stacked with several members who not only oppose the specific surveillance authority set to sunset this year, but also have concerns about the broader Foreign Intelligence Surveillance Act.

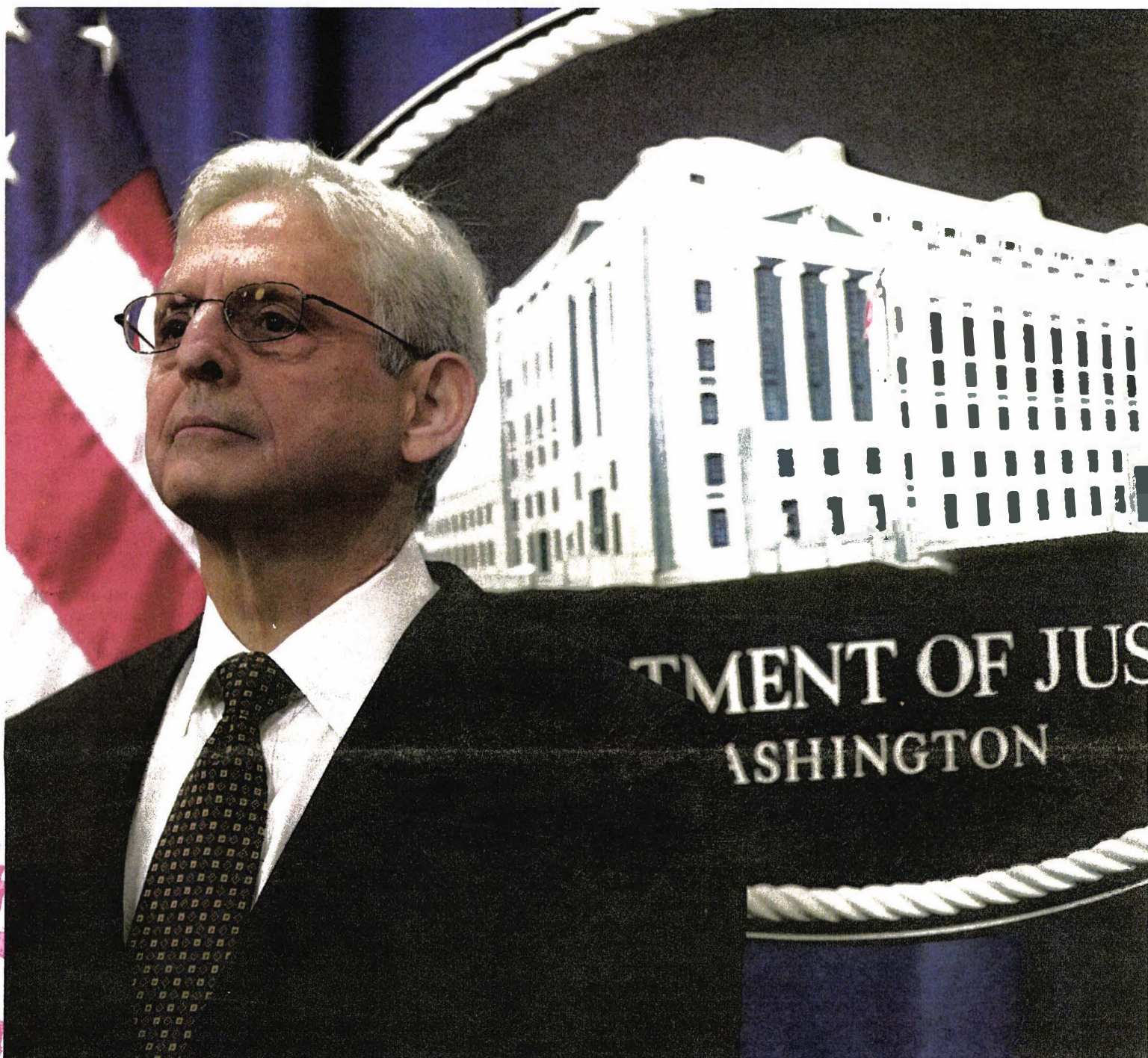
Those calls are being fueled, in part, by a recently declassified report on the use of Section 702 from December 2019 to May 2020. In a sign of the odd political bedfellows who are likely to push reforms, conservative Rep. Andy Biggs (R-Ariz.) and progressive Rep. Pramila Jayapal (D-Wash.), both members of Jordan's panel, vented publicly over a detail tucked into a footnote of the report: An FBI intelligence analyst queried surveillance databases using only the name of a U.S. House member.

The administration is aware it's facing a heavy lift and aren't ruling out changes to the program. Officials have stressed in interviews and in the Tuesday letter to congressional leadership that it is open to potential improvements.

And they're taking initial steps to try to quell a fight on the front end. Biden administration officials' opening pitch is coming much earlier than it did in past years — they estimated they waited until September to begin discussions last time — and they've dropped their pitch for a permanent extension, which lawmakers balked at in 2018. They're also offering to give lawmakers classified briefings to make their case for reauthorization.

But the Biden administration is drawing a red line on an overhaul that would change the essential function of the authority. Director of National Intelligence Avril Haines and Attorney General Merrick Garland, in a letter to congressional leadership, wrote that they needed to "fully preserve its efficacy."

In a second prong of the administration's opening salvo, Assistant Attorney General Matthew Olsen made his pitch for continuing the



CAROLYN KASTER/AP

The administration is drawing a red line on a FISA overhaul that would change the essential function of its section 702 authority. Director of National Intelligence Avril Haines and Attorney General Merrick Garland (above) wrote congressional leadership that they needed to "fully preserve its efficacy."

program during a Brookings Institution event on Tuesday using stark terms.

"What keeps me up at night is thinking about what will happen if we fail to renew Section 702 of FISA," he said.

And Biden administration officials are preemptively pushing back on likely proposals from privacy

timely way potentially critical information."

The administration does have congressional allies, particularly among Senate leadership and members of both the House and Senate Intelligence Committees. Senate Majority Leader Chuck Schumer and Minority Leader Mitch McConnell, as well as the Intelligence

last year. The three Republicans, each on their chamber's Intelligence Committee, want to reauthorize the program, though they are expected to pair that with broader FISA reforms — including in how judges are assigned to surveillance applications.

Rep. Mike Turner (R-Ohio), who chairs the House Intelligence

Trump and Attorney General Bill Barr — led to three unrelated surveillance powers lapsing, critics of Section 702 believe the administration views the program as so critical that they will agree to sweeping changes that might once have been off the table.

The administration is urging lawmakers to stay narrowly focused on Section 702, but officials admit that's unlikely. That's in part because of a high-profile series of reports from DOJ Inspector General Michael Horowitz that found "widespread" noncompliance by the department when it came to a key step in FBI procedure that was designed as a guardrail for ensuring accuracy in surveillance applications.

We are "aware that there are those who want to talk about reforms or changes," said a senior administration official, granted anonymity to speak candidly. "And in the months to come, of course, we anticipate hearing what it is that others who want to have those conversations have in mind."

**John Sakellariadis** and **Alexander Ward** contributed to this report.

**"What keeps me up at night is thinking about what will happen if we fail to renew Section 702 of FISA."**

— Assistant Attorney General Matthew Olsen

advocates who want to change the program. One area that is already coming under early reform chatter is so-called "backdoor" searches, when government agencies sift through already acquired data for information that was "incidentally" collected on Americans. A senior administration official argued that banning or trying to restrict searches involving U.S. persons "would either ban or restrict the government from accessing in a

panel's bipartisan leaders, all voted to reauthorize the program in 2018. Of the 65 lawmakers who previously voted to reauthorize 702, roughly 20 have left the Senate — meaning supporters will need to pick up new allies.

And in a nod to the difficult debate ahead, GOP Reps. Darin LaHood of Illinois, Brian Fitzpatrick of Pennsylvania and Chris Stewart of Utah have quietly been working on the reauthorization effort since

Committee and who tapped the trio to take the lead, echoed their general direction, saying FISA is a "critical tool in our national security arsenal" and that he supports extending it, but "with reforms that will protect American's civil liberties."

But privacy advocates believe they are at a point of maximum leverage. Unlike 2020, when a congressional stalemate — and mixed signals between then-President



U.S. HOUSE OF REPRESENTATIVES  
PERMANENT SELECT COMMITTEE  
ON INTELLIGENCE

March 8, 2023

The Honorable Christopher Wray  
Director  
Federal Bureau of Investigation  
Washington, D.C. 20535

Dear Director Wray:

In preparation for the reauthorization of Title VII of the Foreign Intelligence Surveillance Act (FISA) and reforms to Section 702 and the FISA authorities writ large, a major concern held by both Members of Congress and the American public is the number of U.S. person queries run against unminimized Section 702 collected information. In 2021, after the Department of Justice and the Office of the Director of National Intelligence identified numerous compliance incidents involving the querying of raw FISA information by the FBI, it's my understanding that there were efforts to institute remedial measures to strengthen compliance in this area.

In a memorandum issued by the Department of Justice National Security Division last week, the DOJ summarized these recent remediation efforts. While I fully support the FBI implementing additional guardrails to protect the Constitutional rights of U.S. persons and taking step to remedy the clear flaws in the procedures dictating the querying of Section 702 information, there are still many questions to be answered.

As we read through the expansive collection of information contained within the audit reports provided to the Committee, we are familiar with the large number of compliance incidents, but we are repeatedly faced with case facts which we don't know align with the remedial measures implemented. Lacking much of the factual context to these compliance incidents, but with the goal to determine if the remedial measures now in place would have prevented the incidents from occurring, I respectfully request that the FBI conduct an assessment of all FBI noncompliance incidents contained within the 707 semiannual reports issued to Congress for violations that occurred during calendar year 2019 and 2020, and provide a report to this Committee explaining how the specific incident would or would not have occurred had the now-instituted FBI remedial measures been in place at the time of the incident.

Thank you for your attention to this matter.

Sincerely,

A handwritten signature in blue ink that reads "Michael R. Turner".

Michael R. Turner  
Chairman

cc: The Honorable James A. Himes, Ranking Member  
Permanent Select Committee on Intelligence



Table 1: Lead country and technology monopoly risk.

Technology	Lead country	Technology monopoly risk
<b>Advanced materials and manufacturing</b>		
1. Nanoscale materials and manufacturing	China	high
2. Coatings	China	high
3. Smart materials	China	medium
4. Advanced composite materials	China	medium
5. Novel metamaterials	China	medium
6. High-specification machining processes	China	medium
7. Advanced explosives and energetic materials	China	medium
8. Critical minerals extraction and processing	China	low
9. Advanced magnets and superconductors	China	low
10. Advanced protection	China	low
11. Continuous flow chemical synthesis	China	low
12. Additive manufacturing (incl. 3D printing)	China	low
<b>Artificial intelligence, computing and communications</b>		
13. Advanced radiofrequency communications (incl. 5G and 6G)	China	high
14. Advanced optical communications	China	medium
15. Artificial intelligence (AI) algorithms and hardware accelerators	China	medium
16. Distributed ledgers	China	medium
17. Advanced data analytics	China	medium
18. Machine learning (incl. neural networks and deep learning)	China	low
19. Protective cybersecurity technologies	China	low
20. High performance computing	USA	low
21. Advanced integrated circuit design and fabrication	USA	low
22. Natural language processing (incl. speech and text recognition and analysis)	USA	low
<b>Energy and environment</b>		
23. Hydrogen and ammonia for power	China	high
24. Supercapacitors	China	high
25. Electric batteries	China	high
26. Photovoltaics	China	medium
27. Nuclear waste management and recycling	China	medium
28. Directed energy technologies	China	medium
29. Biofuels	China	low
30. Nuclear energy	China	low
<b>Quantum</b>		
31. Quantum computing	USA	medium
32. Post-quantum cryptography	China	low
33. Quantum communications (incl. quantum key distribution)	China	low
34. Quantum sensors	China	low
<b>Biotechnology, gene technology and vaccines</b>		
35. Synthetic biology	China	high
36. Biological manufacturing	China	medium
37. Vaccines and medical countermeasures	USA	medium
<b>Sensing, timing and navigation</b>		
38. Photonic sensors	China	high
<b>Defence, space, robotics and transportation</b>		
39. Advanced aircraft engines (incl. hypersonics)	China	medium
40. Drones, swarming and collaborative robots	China	medium
41. Small satellites	USA	low
42. Autonomous systems operation technology	China	low
43. Advanced robotics	China	low
44. Space launch systems	USA	low

Note: A visual summary of the top 5 countries for each technology area can be found in [Appendix 1.1](#)

Dear Chairman Turner and Representative Stefanik:

This responds to your request—reflected in the Fiscal Year (FY) 2023 Intelligence Authorization Act (IAA) and in Rep. Stefanik’s letter, dated December 12, 2022—to the Federal Bureau of Investigation (FBI), requesting a copy of the FBI Inspection Division’s (INSD) Internal Review (Internal Review) related to the 2018 tragic limousine crash in Schoharie, New York. This supplements our prior correspondence to Rep. Stefanik, dated April 22, 2022 and November 25, 2022, and our briefing to the House Permanent Select Committee on Intelligence staff, which included a detailed overview of the FBI’s confidential human source program, on May 18, 2022.

The Internal Review is now complete. As a further accommodation to the Committee’s stated oversight objectives, the FBI will provide a briefing by INSD leadership and, in connection with that briefing, will make available the Internal Review with certain redactions, such as those required to protect personally identifiable information, and consistent with our law enforcement and national security obligations. We will coordinate with your staff regarding this in camera review of the materials, which have been Bates number FBI-HPSCI118-INSD-000001 to FBI-HPSCI118-INSD-000023. The FBI is providing this briefing and materials with the understanding that the Committee will not publicly disclose the non-public information contained therein. The production of these materials does not waive any applicable privilege. The FBI considers the provision of the Internal Review as a fulfillment of the above-referenced

Sincerely,

Christopher Dunham  
Acting Assistant Director