



December 30, 2016

**PRESS RELEASE: Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity**  
**ODNI.gov, 29 December 2016**

On October 7, 2016, Secretary Johnson and Director Clapper issued a joint statement that the intelligence community is confident the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations, and that the disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks are consistent with the Russian-directed efforts. The statement also noted that the Russians have used similar tactics and techniques across Europe and Eurasia to influence public opinion there.

Today, DHS and FBI released a Joint Analysis Report (JAR) which further expands on that statement by providing details of the tools and infrastructure used by Russian intelligence services to compromise and exploit networks and infrastructure associated with the recent U.S. election, as well as a range of U.S. government, political and private sector entities.

This activity by Russian intelligence services is part of a decade-long campaign of cyber-enabled operations directed at the U.S. Government and its citizens. These cyber operations have included spearphishing, campaigns targeting government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations; theft of information from these organizations; and the recent public release of some of this stolen information. In other countries, Russian intelligence services have also undertaken damaging and disruptive cyber-attacks, including on critical infrastructure, in some cases masquerading as third parties or hiding behind false online personas designed to cause victim to misattribute the source of the attack. The Joint Analysis Report provides technical indicators related to many of these operations, recommended mitigations and information on how to report such incidents to the U.S. Government.

A great deal of analysis and forensic information related to Russian government activity has been published by a wide range of security companies. The U.S. Government can confirm that the Russian government, including Russia's civilian and military intelligence services, conducted many of the activities generally described by a number of these security companies. The Joint Analysis Report recognizes the excellent work undertaken by security companies and private sector network owners and operators, and provides new indicators of compromise and malicious infrastructure identified during the course of investigations and incident response. The U.S. Government seeks to arm network defenders with the tools they need to identify, detect and disrupt Russian malicious cyber activity that is targeting our country's and our allies' networks.

We encourage security companies and private sector owners and operators to look back within their network traffic for signs of the malicious activity described in the Joint Analysis Report. We also encourage such entities to utilize these indicators in their proactive defense efforts to block malicious cyber activity before it occurs. DHS has already added these indicators to its Automated Indicator

# PIAB Media Highlights

## December 30, 2016

Sharing service, which provides indicators of malicious cyber activity at machine speed. Entities that are participating in this service have already implemented these indicators for the network protection activities.

### **Russia's 'Grizzly Steppe' Cyberattacks Started Simply, U.S. Says**

**Chris Strohm, Bloomberg.com, 29 December 2016**

The attack against U.S. democracy began in the summer of 2015 with a simple trick: Hackers working for Russia's civilian intelligence service sent e-mails with hidden malware to more than 1,000 people working for the American government and political groups.

U.S. intelligence agencies say that was the modest start of "Grizzly Steppe," their name for what they say developed into a far-reaching Russian operation to interfere with this year's presidential election.

Prodded to produce evidence by Russia, which has denied a role in hacking -- and by an openly skeptical President-elect Donald Trump -- the FBI and the Department of Homeland Security did so Thursday. They issued a 13-page joint analysis just as President Barack Obama imposed sanctions against Russian government organizations and individuals and expelled 35 Russian operatives.

While Trump said in a statement Thursday that "it's time for our country to move on to bigger and better things," he said he "will meet with leaders of the intelligence community next week in order to be updated on the facts of this situation." As president-elect he's entitled to see the classified details behind the public report.

#### **Foothold Into DNC**

The initial hackers sent e-mails that appeared to come from legitimate websites and other Internet domains tied to U.S. organizations and educational institutions, according to the report. Those who were fooled into clicking on the "spearphishing" e-mails provided a foothold into the Democratic National Committee -- although the party organization wasn't identified by name in the report -- and key e-mail accounts for material that would later be leaked to damage Hillary Clinton in her losing campaign against Trump.

"This activity by Russian intelligence services is part of a decade-long campaign of cyber-enabled operations directed at the U.S. government and its citizens," according to a joint statement from the Federal Bureau of Investigation, DHS and the Office of the Director of National Intelligence. "The U.S. government seeks to arm network defenders with the tools they need to identify, detect and disrupt Russian malicious cyber activity that is targeting our country's and our allies' networks."

Dmitry Peskov, a Kremlin spokesman, rejected the U.S. conclusions. "We categorically disagree with any of the groundless allegations or charges against Russia," he said on a conference call. "These actions by the current administration in Washington are unfortunately a manifestation of an unpredictable and you could even say aggressive policy."

#### **Malware Code**

In addition to providing evidence, the report was intended to embarrass and stymie the Russian government by making public its tactics, techniques and procedures, according to a U.S. official who asked not to be identified discussing internal deliberations.

Along with the report, the Homeland Security Department released an extensive list of Internet Protocol addresses, computer files, malware code and other "signatures" that it said the Russian hackers have used.

# PIAB Media Highlights

## December 30, 2016

"These actors set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets," the report said.

The initial hackers worked for Russia's FSB, the successor to the Soviet Union's KGB. Once inside the DNC, the group dubbed "Advanced Persistent Threat 29" or "APT 29," used stolen credentials to expand its access to directories and other data, and made off with e-mail from several accounts through encrypted communication channels, according to the report.

### Second Wave

Then, a second wave came in the spring of 2016. Hackers working for Russia's military intelligence service, the GRU, and dubbed "Advanced Persistent Threat 28" or APT 28, infiltrated the DNC's networks through more spearphishing e-mails, the report said.

"This time, the spearphishing e-mail tricked recipients into changing their passwords through a fake webmail domain hosted on APT 28 operational infrastructure," according to the report. "Using the harvested credentials, APT 28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple senior party members. The U.S. government assesses that information was leaked to the press and publicly disclosed."

While the report doesn't name the DNC, U.S. officials and cybersecurity researchers have confirmed that it was a prime target of the Russian hackers.

"A great deal of analysis and forensic information related to Russian government activity has been published by a wide range of security companies," according to the statement from the FBI, DHS and DNI. "The U.S. government can confirm that the Russian government, including Russia's civilian and military intelligence services, conducted many of the activities generally described by a number of these security companies."

### Still Hacking

The U.S. government first announced that intelligence agencies had high confidence that the Russian government was behind the hacking a month before the Nov. 8 election. Despite that public declaration, the hacking attacks have apparently continued.

Actors probably associated with Russian civilian and military intelligence services "are continuing to engage in spearphishing campaigns, including one launched as recently as November 2016, just days after the U.S. election," the report said.

## Obama Strikes Back at Russia for Election Hacking

David E. Sanger, New York Times, 30 December 2016, Page A1

WASHINGTON — President Obama struck back at Russia on Thursday for its efforts to influence the 2016 election, ejecting 35 suspected Russian intelligence operatives from the United States and imposing sanctions on Russia's two leading intelligence services.

The administration also penalized four top officers of one of those services, the powerful military intelligence unit known as the G.R.U. Intelligence agencies have concluded that the G.R.U. ordered the attacks on the Democratic National Committee and other political organizations, with the approval of the Kremlin, and ultimately enabled the publication of the emails it harvested.

## PIAB Media Highlights

### December 30, 2016

The expulsion of the 35 Russians, whom the administration said were spies posing as diplomats and other officials, and their families was in response to the harassment of American diplomats in Russia, State Department officials said. It was unclear if they were involved in the hacking.

In addition, the State Department announced the closing of two waterfront estates — one in Glen Cove, N.Y., and another on Maryland's Eastern Shore — that it said were used for Russian intelligence activities, although officials declined to say whether they were specifically used in the election-related hacks.

Taken together, the sweeping actions announced by the White House, the Treasury, the State Department and intelligence agencies on Thursday amount to the strongest American response yet to a state-sponsored cyberattack. They also appeared intended to box in President-elect Donald J. Trump, who will now have to decide whether to lift the sanctions on Russian intelligence agencies when he takes office next month.

Mr. Trump responded to the Russian sanctions late Thursday by reiterating a call to "move on." But he pledged to meet with intelligence officials, who have concluded that the Russian hacking was an attempt to tip the election to Mr. Trump.

In an earlier statement from Hawaii, Mr. Obama took a subtle dig at Mr. Trump, who has consistently cast doubt on the intelligence showing that the Russian government was deeply involved in the hacking. "All Americans should be alarmed by Russia's actions," Mr. Obama said, and added that the United States acted after "repeated private and public warnings that we have issued to the Russian government, and are a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior."

He issued a new executive order that allows him, and his successors, to retaliate for efforts to influence elections in the United States or those of "allies and partners," a clear reference to concern that Russia's next target may be Germany and France. Already there are reports of influence operations in both.

Mr. Trump's position is at odds with most members of his party, who after classified briefings have called for investigations into the combination of cyberattacks and old-style information warfare used in the 2016 campaign. Mr. Trump has largely stuck to the theory he set forth in a debate with Hillary Clinton in September, when he said the hacks could have been organized by "somebody sitting on their bed that weighs 400 pounds."

Russia criticized the sanctions and vowed retaliation.

"Such steps of the U.S. administration that has three weeks left to work are aimed at two things: to further harm Russian-American ties, which are at a low point as it is, as well as, obviously, deal a blow on the foreign policy plans of the incoming administration of the president-elect," Dmitri S. Peskov, the spokesman for President Vladimir V. Putin, told reporters.

Konstantin Kosachyov, the head of the foreign affairs committee in the upper house of the Russian Parliament, told Interfax that "this is the agony not even of 'lame ducks,' but of 'political corpses.'"

Despite the international fallout and political repercussions surrounding the announcement, it is not clear how much effect the sanctions will have, except on the ousted diplomats, who have until midday Sunday to leave the country. G.R.U. officials rarely travel to the United States, or keep assets here.

The four Russian intelligence officials are Igor Valentinovich Korobov, the chief of the G.R.U., and three deputies: Sergey Aleksandrovich Gizunov, Igor Olegovich Kostyukov and Vladimir Stepanovich Alexseyev.

## PIAB Media Highlights

### December 30, 2016

The administration also put sanctions on three companies and organizations that it said supported the hacking operations: the Special Technology Center, a signals intelligence operation in St. Petersburg, Russia; a firm called Zorsecurity that is also known as Esage Lab; and the Autonomous Noncommercial Organization Professional Association of Designers of Data Processing Systems, whose lengthy name, American officials said, was cover for a group that provided special training for the hacking.

Still, the sanctions go well beyond the modest sanctions imposed against North Korea for its attack on Sony Pictures Entertainment two years ago, which Mr. Obama said at the time was an effort to repress free speech — a somewhat crude comedy, called “The Interview,” imagining a C.I.A. plot to assassinate Kim Jung-un, the country’s leader.

The sanctions are not as biting as previous ones in which the United States and its Western allies took aim at broad sectors of the Russian economy and blacklisted dozens of people, some of them close friends of Mr. Putin’s. Those sanctions were in response to the Russian annexation of Crimea and its activities to destabilize Ukraine. Mr. Trump suggested in an interview with The New York Times this year that he believed those sanctions were useless, and left open the possibility he might lift them.

The F.B.I. and the Department of Homeland Security on Thursday also released samples of malware and other indicators of Russian cyberactivity, including network addresses of computers commonly used by the Russians to start attacks. But the evidence in a report, in which the administration referred to the Russian cyberactivity as Grizzly Steppe, fell short of anything that would directly tie senior officers of the G.R.U. or the F.S.B., the other intelligence service, to a plan to influence the election.

A more detailed report on the intelligence, ordered by Mr. Obama, will be published in the next three weeks, though much of the information — especially evidence collected from “implants” in Russian computer systems, tapped conversations and spies — is expected to remain classified.

Several Obama administration officials, including Vice President Joseph R. Biden Jr., have suggested that there may also be a covert response, one that would be obvious to Mr. Putin but not to the public.

While that may prove satisfying, many outside experts have said that unless the public response is strong enough to impose a real cost on Mr. Putin, his government and his vast intelligence apparatus, it might not deter further activity.

“They are concerned about controlling retaliation,” said James A. Lewis, a cyberexpert at the Center for Strategic and International Studies in Washington.

But John P. Carlin, who recently left the administration as the chief of the Justice Department’s national security division, where he assembled cases against North Korean, Chinese and Iranian hackers, called the administration’s actions a “significant step that is consistent with a new model: When you violate norms of behavior in this space, we can figure out who did it and we can impose consequences.”

The Obama administration was riven for months by an internal debate about how much of its evidence to make public. In interviews for a New York Times investigation into the hack, several of Mr. Obama’s top aides expressed regret that they had not made evidence public earlier, or reacted more strongly. None said they believed it would have affected the outcome of the election, however.

In recent weeks, Mr. Obama decided that the authorities he created in April 2015 to retaliate against states or individuals that conduct hacking after the Sony attack did not go far enough. They made no provision issuing sanctions in response to an incursion on the electoral system — an attack few saw coming.

So he ordered his lawyers to amend the executive order, specifically giving himself and his successor the authority to issue travel bans and asset freezes on those who “tamper with, alter, or cause a

## PIAB Media Highlights

### December 30, 2016

misappropriation of information, with a purpose or effect of interfering with or undermining election processes or institutions.”

The administration has not publicly criticized how its own officials handled the case. But the Times investigation revealed that the F.B.I. first informed the Democratic National Committee that it saw evidence that the committee’s email systems had been hacked in the fall of 2015. Months of fumbling and slow responses followed.

Mr. Obama said at a news conference that he was first notified early this summer. But one of his top aides met Russian officials in Geneva to complain about activity in April.

By the time the leadership of the committee woke up to what was happening, the G.R.U. had not only obtained emails through a hacking group that has been closely associated with it for years, but, investigators say, also allowed them to be published on a number of websites, including a newly created one called DC Leaks and the far more established WikiLeaks. Meanwhile, several states reported the “scanning” of their voter databases — which American intelligence agencies also attributed to Russian hackers. But there is no evidence, American officials said, that Russia sought to manipulate votes or voter rolls on Nov. 8.

Mr. Obama decided not to issue sanctions earlier for fear of Russian retaliation ahead of Election Day. Some of his aides now believe that was a mistake. But the president made clear before leaving for Hawaii that he planned to respond.

Neil MacFarquhar contributed reporting from Moscow.

## **How Russia Recruited Elite Hackers for Its Cyberwar**

**Andrew E. Kramer, New York Times, 30 December 2016, Page A1**

MOSCOW — Aleksandr B. Vyarya thought his job was to defend people from cyberattacks until, he says, his government approached him with a request to do the opposite.

Mr. Vyarya, 33, a bearded, bespectacled computer programmer who thwarted hackers, said he was suddenly being asked to join a sweeping overhaul of the Russian military last year. Under a new doctrine, the nation’s generals were redefining war as more than a contest of steel and gunpowder, making cyberwarfare a central tenet in expanding the Kremlin’s interests.

“Sorry, I can’t,” Mr. Vyarya said he told an executive at a Russian military contracting firm who had offered him the hacking job. But Mr. Vyarya was worried about the consequences of his refusal, so he abruptly fled to Finland last year, he and his former employer said. It was a rare example of a Russian who sought asylum in the face of the country’s push to recruit hackers.

“This is against my principles — and illegal,” he said of the Russian military’s hacking effort.

While much about Russia’s cyberwarfare program is shrouded in secrecy, details of the government’s effort to recruit programmers in recent years — whether professionals like Mr. Vyarya, college students, or even criminals — are shedding some light on the Kremlin’s plan to create elite teams of computer hackers.

American intelligence agencies say that a team of Russian hackers stole data from the Democratic National Committee during the presidential campaign. On Thursday, the Obama administration imposed sanctions against Russia for interfering in the election, the bedrock of the American political system.

## PIAB Media Highlights

### December 30, 2016

The sanctions take aim at Russia's main intelligence agencies and specific individuals, striking at one part of a sprawling cyberespionage operation that also includes the military, military contractors and teams of civilian recruits.

For more than three years, rather than rely on military officers working out of isolated bunkers, Russian government recruiters have scouted a wide range of programmers, placing prominent ads on social media sites, offering jobs to college students and professional coders, and even speaking openly about looking in Russia's criminal underworld for potential talent.

Those recruits were intended to cycle through military contracting companies and newly formed units called science squadrons established on military bases around the country.

As early as 2013, Sergei K. Shoigu, the Russian defense minister, told university rectors at a meeting in Moscow that he was on a "head hunt in the positive meaning of the word" for coders.

The Defense Ministry bought advertising on Vkontakte, Russia's most popular social network. One video shows a man clanging a military rifle on a table beside a laptop computer, then starting to type.

"If you graduated from college, if you are a technical specialist, if you are ready to use your knowledge, we give you an opportunity," the ad intoned. Members of the science squadrons, the video said, live in "comfortable accommodation," shown as an apartment furnished with a washing machine.

University students subject to mandatory conscription in the nation's armed forces, but who wanted to avoid brutal stints as enlistees, could opt instead to join a science squadron. A government questionnaire asks draftees about their knowledge of programming languages.

The ministry posted openings on job forums, according to an investigation by Meduza, a Russian news site based in Riga, Latvia, that first disclosed the recruitment effort. One post from 2014 advertised for a computer scientist with knowledge of "patches, vulnerabilities and exploits," which refers to sabotage used to alter a computer.

Given the size of Russia's cybercrime underworld, it was not long before the military considered recruiting those it described as "hackers who have problems with the law."

In an article titled "Enlisted Hacker" in Rossiiskaya Gazeta, the government newspaper, a deputy minister of defense, Gen. Oleg Ostapenko, said the science squadrons might include hackers with criminal histories. "From the point of view of using scientific potential, this is a matter for discussion," he was quoted as saying in 2013.

Experts say the strategy was more than just talk.

"There have been cases where cybercriminals are arrested but never ended up in prison," said Dmitri Alperovitch, the co-founder and chief technology officer of CrowdStrike, the cybersecurity company that first identified the group known as Fancy Bear as the perpetrator of the Democratic National Committee hacking.

Mr. Vyarya, the programmer who turned down the government's job offer, was an attractive recruit from the opposite end of the spectrum: someone with a career protecting people against hackers.

Specifically, he had experience shielding websites from a maneuver called a distributed denial of service, or DDoS attack, in which the sites are overwhelmed and disabled by a torrent of fake traffic. Among his clients were Vedomosti, an independent newspaper; TV Rain, an opposition-leaning television station; and the website of Aleksei A. Navalny, the opposition leader.

## PIAB Media Highlights

### December 30, 2016

Mr. Vyarya said that in 2015 he was invited to accompany Vasily Brovko, an executive at the military contracting company Rostec, on a trip to Sofia, Bulgaria. But he said it turned out to be a demonstration of a new software suite capable of staging DDoS attacks.

The Bulgarian firm demonstrating the software briefly crashed the website of Ukraine's Defense Ministry and Slon.ru, a Russian news website, Mr. Vyarya said. Slon.ru has confirmed its site went down inexplicably for about two minutes that day, Feb. 5, 2015.

After the demonstration, Mr. Vyarya said Mr. Brovko asked him how the program might be improved. Then, according to Mr. Vyarya, Mr. Brovko offered him a job running the DDoS software, which he said the Russians planned to buy from the Bulgarians for about \$1 million.

Mr. Vyarya said his problems began when he turned down the offer: He was surveilled, and an acquaintance in law enforcement advised him to flee the country. He left in August 2015 for Finland to seek asylum, he and his former employer said. The Finnish government, citing safety and privacy concerns, would not comment on the asylum application.

"As soon as we saw what was on the table, Sasha was given direct instructions to return to his hotel and stop all contacts," said his former boss, Aleksandr V. Lyamin of Qrator, a cyberdefense company in Moscow, using Mr. Vyarya's Russian nickname. But the overtures from the military contractor persisted, Mr. Lyamin said, and Mr. Vyarya fled.

Rostec strongly denied Mr. Vyarya's account. Mr. Brovko did travel to Bulgaria with Mr. Vyarya, the company said, but to evaluate software for defensive, not offensive, cybersystems. A spokeswoman for Mr. Brovko called the account of crashing sites in a product demonstration the imagination of a "mentally unstable" man.

The military's push into cyberwarfare had intensified in 2012, with the appointment of a new minister of defense, Mr. Shoigu. The next year, a senior defense official, Gen. Valery V. Gerasimov published what became known as the Gerasimov Doctrine. It posited that in the world today, the lines between war and peace had blurred and that covert tactics, such as working through proxies or otherwise in the shadows, would rise in importance.

He called it "nonlinear war." His critics called it "guerrilla geopolitics."

But Russia is certainly not alone.

"Almost all developed countries in the world, unfortunately, are creating offensive capabilities, and many have confirmed this," said Anton M. Shingarev, a vice president at Kaspersky, a Russian antivirus company.

Recruitment by Russia's military should be expected, he said. "You or I might be angry about it, but, unfortunately, it's just reality. Many countries are doing it. This is the reality."

American intelligence agencies, including the National Security Agency, have for decades recruited on college campuses. In 2015, the N.S.A. offered a free summer camp to 1,400 high school and middle school students, where they were taught the basics of hacking, cracking and cyberdefense.

In Russia, recruiters have looked well beyond the nation's school system.

In 2013, as Russia's recruitment drive was picking up, Dmitry A. Artimovich, a soft-spoken physicist, was awaiting trial in a Moscow jail for designing a computer program that spammed email users with advertisements for male sexual enhancement products.



## PIAB Media Highlights

### December 30, 2016

One day a cellmate, who had been convicted of selling narcotics online, sidled up to him with some news. The cellmate said that people incarcerated for cybercrimes could get out before trial, in exchange for working for the government. Another inmate had already taken a deal, he said.

"It was an offer to cooperate," Mr. Artimovich said.

"Why else would you work for the government?" he added. "The salaries are tiny. But if you do something illegal, and go to prison for eight or nine years, the F.S.B. can help you," he said, using a Russian abbreviation for the Federal Security Service.

Mr. Artimovich said he decided to take his chances at trial, and served a year in a penal colony.

As Russia ramped up its abilities, government agencies were also in the market for surveillance and hacking software, including some from legal suppliers in the West.

In 2014, a Russian company called Advanced Monitoring that has a license to work with the F.S.B., the agency that succeeded the K.G.B. after the fall of the Soviet Union, bought iPhone hacking software from an Italian company called Hacking Team, according to invoices published by WikiLeaks. Hacking Team has since lost its export license.

Western cybersecurity analysts believe they have identified the one responsible for the breaching the Democratic National Committee: a group nicknamed Fancy Bear.

First known as Advanced Persistent Threat 28, the group has been active since 2007 but its abilities evolved to emphasize attacks, rather than gather intelligence, after the military placed a priority on cyberwarfare.

It stepped up "faketivist" actions that released stolen data through contrived online personalities like Guccifer 2 and websites like DCLeaks, according to Kyle Ehmke, a senior intelligence researcher at ThreatConnect, a cybersecurity company. The group had been called Pawn Storm, named for a chess maneuver. It was nicknamed Fancy Bear in 2014.

This year, the group appropriated the nickname for its own use, setting up the website fancybear.net and publishing hacked data from the World Anti-Doping Agency, which showed that many American athletes, including the American tennis star Serena Williams, had medical exemptions to take banned substances. The hacking was apparently in retaliation for revelations of Russian doping in sports.

President Vladimir V. Putin has said repeatedly, most recently at his annual year-end news conference, that the information released in the recent hacking of the Democratic National Committee was more important than who was behind them.

"The main thing, to my mind, is the information the hackers provided," Mr. Putin said of this summer's cyberattack.

Democratic Party members and the Obama administration should not look abroad for someone to blame for losing the election, Mr. Putin said. "You need to learn how to lose gracefully," he said.

## **Five myths about the President's Daily Brief**

**David Priess, WashingtonPost.com, 29 December 2016**

David Priess, a former analyst and daily intelligence briefer at the CIA, is the author of "The President's Book of Secrets: The Untold Story of Intelligence Briefings to America's Presidents From Kennedy to Obama."

# PIAB Media Highlights

## December 30, 2016

We've learned that President-elect Donald Trump has declined many intelligence briefings, delegating the daily task instead to Vice President-elect Mike Pence. "I get it when I need it," Trump said. "I'm, like, a smart person. I don't need to be told the same thing and the same words every single day for the next eight years." In some ways this is a departure from the approach of past presidents. But there's also widespread misunderstanding of the President's Daily Brief (PDB) and the traditions surrounding it. Here are five erroneous beliefs worth correcting.

### Myth No. 1

The PDB has traditionally been for the president's eyes only.

The very title of this top-secret intelligence report says so: It's the president's book. And indeed, it is tailored to each president's individual needs. CIA officers in 1961 designed what was initially known as the President's Intelligence Checklist specifically for John F. Kennedy's tastes, using punchy words and phrases while avoiding clunky bureaucratic language and annoying classification markings. That checklist evolved into the President's Daily Brief in late 1964, as the agency reformatted and retitled the book of secrets to appeal to Lyndon Johnson's preferences. While the name has stuck, the content and format have continued to evolve. President Obama receives his in digital form and reads it on a tablet.

But while through most of its history the document has been marked "For the President's Eyes Only," the PDB has never gone to the president alone. The most restricted dissemination was in the early 1970s, when the book went only to President Richard Nixon and Henry Kissinger, who was dual-hatted as national security adviser and secretary of state. In other administrations, the circle of readers has also included the vice president, the secretary of defense and the chairman of the Joint Chiefs of Staff, along with additional White House staffers. By 2013, Obama's PDB was making its way to more than 30 recipients, including the president's top strategic communications aide and speechwriter, and deputy secretaries of national security departments.

### Myth No. 2

Senior intelligence officers have briefed past presidents in person every day.

The commander in chief has received the PDB every working morning for the past 50 years. In-person briefings, though, haven't been as frequent.

Presidents Gerald Ford, George H.W. Bush (previously a CIA director) and George W. Bush wanted face-to-face briefings daily. But they stand out as the exceptions. Johnson and Nixon rarely saw their CIA directors or senior intelligence officers for anything, much less to brief the PDB. Presidents Jimmy Carter and Ronald Reagan discussed the daily book with their national security advisers, not CIA officers. Presidents Bill Clinton and Obama received in-person presentations, but irregularly. Taken together, institutionalized daily briefings have occurred during less than 15 years of the PDB's half-century.

Former defense secretary Bob Gates, who has had insight into the use of the PDB by almost every president since Johnson, told me that "one of the greatest values of the PDB is the interaction with the president, which allows the leadership of CIA and the community to have a better idea of what's on the president's mind, where he is coming from on issues, what's on his agenda and what he needs to know." But most often feedback has been in response to the written product and conveyed through the national security adviser.

### Myth No. 3

Presidents get most of their information on intelligence and national security from the PDB.

# PIAB Media Highlights

## December 30, 2016

Vice President Dick Cheney, arguing that PDBs should be kept out of the hands of 9/11 investigators, called them “the family jewels.” Observers often speak as if the president wouldn’t know anything about global developments without them. And they put inordinate weight on what appeared in the daily book around the time of a national security incident. For example, the House Select Committee on Benghazi investigated Obama’s PDBs in the days around Sept. 11, 2012, to find out what and how he was told about the attack in that Libyan city.

The intelligence assessments in the PDB, however, are just one slice of a very large pie. Important information makes its way to the president throughout the day, especially during crises, from a variety of channels: meetings with top West Wing advisers, messages from the White House Situation Room, phone calls from national security officials and in-person intelligence briefings that extend beyond the material in the once-per-day PDB.

During the Cuban missile crisis, for example, Kennedy was briefed on Cuba in frequent meetings at the White House. His daily intelligence document kept him up to speed on other world events but largely neglected Cuba itself during those 13 days. Similarly, Johnson in early 1965 started receiving a daily Vietnam report from the CIA, obviating the need for the PDB to cover every detail on that topic as the war expanded.

### Myth No. 4

Presidents have placed enormous weight on the PDB.

As the ultimate product of the intelligence community’s collection and analytic efforts, the PDB tends to command respect, as some presidential comments reflect. Speaking with Trevor Noah on “The Daily Show” on Dec. 12, Obama implied that without the PDB, he would be “flying blind.” Clinton told me that even on an uneventful day, he got 90 percent of what he needed to make good decisions across a range of issues from the daily document. “I can’t imagine any president not taking it seriously, not reading it carefully,” he said.

But several presidents have also pointed out the PDB’s flaws and inconsistencies. Less than two months into his term, President Jimmy Carter told intelligence officials that he was “disappointed” with the analysis he received and wanted more “divergent views.” And in November 1978, as protests in Iran against U.S. ally Shah Mohammad Reza Pahlavi spiraled out of control, Carter sent a blistering note to his national security team lamenting the “quality of our political intelligence.” The PDB also exasperated Clinton — “all the time,” he told me — because he wanted more than it could provide. He even told the 9/11 Commission in April 2004 that he found the Secretary’s Morning Summary from the State Department’s Bureau of Intelligence and Research more helpful than the PDB in providing context for developments overseas.

Of all the presidents in the past 50 years, Nixon placed the least emphasis on the book. “The PDB was not a central document in our thinking,” Kissinger told me. “It was one input.” Nixon’s distrust of the CIA prompted him to undervalue most of the agency’s judgments, if he read them at all. In a meeting of the National Security Council in June 1969, he accused analysts of trying to use intelligence to support conclusions, rather than to make conclusions. He didn’t offer any direct feedback on a single PDB item during more than 5 1 / 2 years in office.

### Myth No. 5

The PDB isn’t worth the president’s time.

The PDB contains timely and, hopefully, accurate assessments of national security threats and foreign policy opportunities. Each article, drafted by CIA analysts — and, since post-9/11 reforms kicked in more fully in 2005, by their colleagues across the intelligence community — synthesizes classified and

## PIAB Media Highlights

### December 30, 2016

unclassified source material into an assessment that is usually no longer than a single page, focused on what the president needs to know rather than what he wants to hear. But does the PDB really repeat things “every single day” for the busiest man in the world?

A newcomer to analysis could be forgiven for underestimating the value of successive articles about the same country, region or city that share similar probabilistic and estimative language. But the slight distinctions from one report to the next often provide the best decision advantage for the president, whether he’s smart or not. As Obama explained in an interview last January, when he goes through the PDB, “I’m looking at: Are there significant differences?” The PDB’s insights into what other governments, groups and individuals around the globe are doing or considering doing — even if only marginally different than in the days or weeks before — help the commander in chief get ahead of crises before they develop or react to them more confidently if they do erupt. Even when the text seems repetitive, there’s value in such incremental updates. Clinton, for example, told me there were few days when he felt he got nothing out of the PDB.