

protests and carrying out cyberattacks. (On Thursday, Gavrilița announced her resignation after 18 months in power.) According to her, last year Moldova suffered from the biggest cyberattacks in its history. The country has also been on the receiving end of frequent bomb threats, receiving fake emails, many of which were sent from Russian and Belarusian IP addresses, warning of bomb threats at more than 50 facilities across the country, including the airport, the capital's City Council, the Parliament, and various ministries. As of September, Moldovan security agencies recorded 148 bomb alerts against 885 state institutions in 2022. Over the past year, Moldova has also witnessed a sharp increase in cyberattacks. In August, the pro-Russian hacker group Killnet announced a week-long hacking campaign against Moldova. In October, hackers targeted 80 Moldovan state computer systems with distributed denial-of-service (DDoS) attacks. In November, a newly-registered website called Moldova Leaks released private Telegram conversations purportedly involving prominent Moldovan political figures, sparking a political scandal. The Moldovan president's office claimed the content of the conversations was fake, but the leak indicates the probable interference of Russian hackers and intelligence services in the country's internal politics. In January, Moldova's government institutions were hit by a wave of phishing attacks — hackers sent more than 1,330 emails to accounts belonging to the country's state services. Its internet connection is also suffering from the war in Ukraine. In November, Russian missile strikes on Ukraine caused internet disruptions in Moldova, as it is connected to Ukraine's power grid. *Gavrilița said that Russia's invasion put Moldova's economy, energy security, and social stability under great strain.* ([Recorded Future](#))

Disinformation Narratives Related to Sweden and Finland's NATO Applications: Throughout Russia's war on Ukraine, the Kremlin's disinformation efforts have sought to craft and disseminate false narratives that serve several political goals and influence public opinion about the conflict. Since April 2022, Russian-backed information manipulation networks online have sought to seed and amplify a number of false narratives regarding Sweden and Finland's NATO application, which was formally submitted on May 18, 2022. Many of the false or misleading narratives targeting Sweden are centered around sensitive and polarizing topics in the country related to immigration, Islamophobia, and far-right conspiracy theories. *According to Washington-based think tank monitoring, between September 27 - October 3, 2022, posts alleging that the U.S. was responsible for the sabotage of Nord Stream pipelines increased by 15,000% across 25 social media platforms compared to the week prior.* ([IntelBrief: The Soufan Center](#))

Twitter under fire in Europe: [Wired](#) is reporting that Twitter is blatantly ignoring the EU's GDPR legislation by ignoring requests from users to have their data deleted from the platform. Moreover, The European Commission [singled out Twitter](#) as lagging behind Google, Meta, Microsoft, Twitch, and TikTok when it came to efforts to tackle disinformation. ([Reuters](#))

Google to expand misinformation prebunking in Europe: After seeing promising results in Eastern Europe, Google will initiate a new campaign in Germany that aims to make people more resilient to the corrosive effects of online misinformation. The tech giant plans to release a series of short videos highlighting the techniques common to many misleading claims. The videos will appear as advertisements on platforms like Facebook, YouTube or TikTok in Germany. A similar campaign in India is also in the works. It's an approach called prebunking, which involves teaching people how to spot false claims before they encounter them. The strategy is gaining support among researchers and tech companies. ([Seattle Times](#))

EU publishes first Foreign Information Manipulation and Interference report: The European External Action Service (EEAS) says it detected and analyzed 100 FIMI events between October and December 2022. Most of these targeted Russia's invasion of Ukraine. In 60 of the 100 incidents, the threat actors used misinformation and disinformation in an attempt to show support for Russia's invasion. Furthermore, the report found that the Russian government itself and its diplomatic channels were part of the FIMI events, spreading false information and trying to control narratives. In addition, Russian threat actors also used impersonation attacks, either posing as foreign officials or foreign news outlets in an attempt to spread their agenda. Most interestingly, however, is the EEAS aim *to provide the defender community with a proof-of-concept for a common framework that enables mutual sharing of complex insights in a timely fashion and at scale*. This is done to create a common understanding and formulate a collective, systematic response to FIMI. ([EU vs. Disinfo](#))

Growing Counterintelligence Concerns in Europe: Recent reporting [from NBC](#) covers the claims of a mole inside the ranks of Germany's BND and some historical analysis of Russian intelligence operations in Germany. Additionally, for your reference are other more notable events concerning Russian intelligence operations in 2022, specifically GRU illegals uncovered in [Italy](#) and [Slovakia](#).

European Aviation Ransomware Snapshot: EUROCONTROL, a European civil-military organization dedicated to supporting European aviation, has [published](#) a one-page "data snapshot" that looks at ransomware targeting the aviation supply chain. Globally, EUROCONTROL says "we are aware of approximately 2.5 reported ransomware attacks per week on aviation-related organisations". The good news is that incident reporting is improving and since 2021 EUROCONTROL has a clearer idea of the scale of the problem as information about more incidents are being shared with its CERT. *Although it looks like there may be a small downward trend, the report cautions that this is likely just a side-effect of the invasion of Ukraine.* EUROCONTROL expect to see an increase in ransomware incidents in 2023.

U.S. Cyber Policy and Issues

The Autocrat in Your iPhone: Attached is great Foreign Affairs article which contextualizes citizen labs technical research on mercenary (or commercial) spyware and its implications to democracy. You'll find a plethora of unclassified examples to reference, as needed.

US and UK sanction Trickbot members: The governments of [the United States](#) and [the United Kingdom](#) have levied sanctions against seven Russian nationals for their role in the Trickbot cybercrime gang. Both countries said the sanctions are part of a coordinated crackdown against the ransomware ecosystem. The Trickbot gang, also known as Wizard Spider, is primarily known for its eponymous Trickbot malware botnet. The US and UK sanctions announcements also include the first formal statement linking the Trickbot gang with the Russian government. *Both the US and UK governments say that members of the Trickbot gang are also associated and maintain links to Russian intelligence services, "from whom they have likely received tasking."*

- In the past, Trickbot has rented access to computers infected by its malware to the Ryuk cybercrime group, which deployed its ransomware on corporate or government networks. In addition, Trickbot also developed its own ransomware strains, known as Conti and Diavol, which they also deployed on systems that were previously infected by their botnet. The UK government said that in the UK alone, 149 organizations paid at least £27 million following attacks with the Conti and Ryuk ransomware

strains. "There were 104 UK victims of the Conti strain who paid approximately £10 million and 45 victims of the Ryuk strain who paid approximately £17 million."

- Over the years, the Trickbot botnet has grown to become one of the largest malware operations to date, and the gang's sub-group tasked with carrying out ransomware attacks has become one of the most despised ransomware gangs today after repeatedly targeting medical and healthcare facilities and disrupting their operations—even during the COVID-19 pandemic. *"Members of the Trickbot Group publicly gloated over the ease of targeting the medical facilities and the speed with which the ransoms were paid to the group."*
- With Trickbot's inclusion on the sanctioned entities list, US and UK companies are now forbidden from paying ransoms to the group, and financial entities are mandated to freeze any of the group's assets. Sanctions have proven very successful against ransomware gangs in the past, with the sanctions imposed against EvilCorp in 2019 effectively destroying their ransomware operation (Bitpaymer, Hades, WastedLocker) and making the group and its members pariahs in the cybercrime underground.
- The US Justice Department has also charged Trickbot's Kovalev with conspiracy to commit bank fraud and eight counts of bank fraud in connection with a series of intrusions into victim bank accounts that occurred in 2009 and 2010.
- In response, according to the Russian outlet Govorit Moskva, which sources its story to TASS, *the Duma is considering legal immunity for "hackers acting in the interest of Russia."* Alexander Khinshtein, head of the Duma committee on information policy, said last week, "We are talking about, in general, working out the exemption from liability of those persons who act in the interests of the Russian Federation in the field of computer information both on the territory of our country and abroad." The details will be made public once they're worked out.

East Asia Cyber Policy and Issues

South Korea slaps first independent sanctions on North Korea's cyber activities: South Korea announced on Friday its first independent sanctions on North Korea to counter its illicit cyber activities. Such activities are believed to be used to fund the country's weapons of mass destruction program. *North Korean hackers stole over \$1.2 billion in virtual assets since 2017*, including \$626 million in 2022 alone, according to data released by the Foreign Ministry. "As North Korea's annual exports have decreased by about 100 billion won recently, it has been stealing virtual assets from all over the world, including developing countries and countries friendly to North Korea," said Lee. "This measure is an effort to protect not only our national security, but also the assets of people around the globe." ([Yonhap](#), [Korea JoongAng](#))

North Korea extorts hospitals to fund espionage: North Korea is deploying ransomware in the health care sector to supplement cyber ops against the U.S. and South Korean governments, according to a joint alert released Thursday from multiple U.S. and South Korean agencies. Furthermore, the alert from the National Security Agency, FBI, Cybersecurity and Infrastructure Security Agency, Department of Health and Human Services, the Republic of Korea's Defense Security Agency and the National Intelligence Service warns that Pyongyang is using the illicit cryptocurrencies obtained from the attacks to support state-backed espionage operations that target U.S. defense networks and the defense industrial base. *Separate, but related, a December ransomware attack has led to a massive data breach from California health network.* ([Cyberscoop](#), [Recorded Future](#))

FOREIGN AFFAIRS

JANUARY/FEBRUARY 2023 • VOLUME 102 • NUMBER 1

The Autocrat in Your iPhone

How Mercenary Spyware
Threatens Democracy

RONALD J. DEIBERT

Copyright © 2023 by the Council on Foreign Relations, Inc. All rights reserved. To request permission to distribute or reprint this article, please visit [ForeignAffairs.com/Permissions](https://www.cfr.org/permissions).

The Autocrat in Your iPhone

How Mercenary Spyware Threatens Democracy

RONALD J. DEIBERT

In the summer of 2020, a Rwandan plot to capture exiled opposition leader Paul Rusesabagina drew international headlines. Rusesabagina is best known as the human rights defender and U.S. Presidential Medal of Freedom recipient who sheltered more than 1,200 Hutus and Tutsis in a hotel during the 1994 Rwandan genocide. But in the decades after the genocide, he also became a prominent U.S.-based critic of Rwandan President Paul Kagame. In August 2020, during a layover in Dubai, Rusesabagina was lured under false pretenses into boarding a plane bound for Kigali, the Rwandan capital, where government authorities immediately arrested him for his affiliation with an opposition group. The following year, a Rwandan court sentenced him to 25 years in prison, drawing the condemnation of international human rights groups, the European Parliament, and the U.S. Congress.

RONALD J. DEIBERT is Professor of Political Science and Director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy.



Illustration by Daniel Stolle

Less noted at the time, however, was that this brazen cross-border operation may also have employed highly sophisticated digital surveillance. After Rusesabagina's sentencing, Amnesty International and the Citizen Lab at the University of Toronto, a digital security research group I founded and direct, discovered that smartphones belonging to several of Rusesabagina's family members who also lived abroad had been hacked by an advanced spyware program called Pegasus. Produced by the Israel-based nso Group, Pegasus gives an operator near-total access to a target's personal data. Forensic analysis revealed that the phone belonging to Rusesabagina's daughter Carine Kanimba had been infected by the spyware around the time her father was kidnapped and again when she was trying to secure his release and was meeting with high-level officials in Europe and the U.S. State Department, including the U.S. special envoy for hostage affairs. nso Group does not publicly identify its government clients and the Rwandan government has denied using Pegasus, but strong circumstantial evidence points to the Kagame regime.

In fact, the incident is only one of dozens of cases in which Pegasus or other similar spyware technology has been found on the digital devices of prominent political opposition figures, journalists, and human rights activists in many countries. Providing the ability to clandestinely infiltrate even the most up-to-date smartphones—the latest “zero click” version of the spyware can penetrate a device without any action by the user—Pegasus has become the digital surveillance tool of choice for repressive regimes around the world. It has been used against government critics in the United Arab Emirates (UAE) and pro-democracy protesters in Thailand. It has been deployed by Mohammed bin Salman's Saudi Arabia and Viktor Orban's Hungary.

But the use of spyware is hardly limited to the world's authoritarians. As researchers have revealed, over the past decade many democracies, including Spain and Mexico, have begun using spyware, as well, in ways that violate well-established norms of human rights and public accountability. U.S. government documents disclosed by *The New York Times* in November 2022 show that the FBI not only acquired spyware services from nso, possibly for counterintelligence purposes, but also contemplated deploying them, including on U.S. targets. (An FBI spokesperson told the *Times* that “there has been no operational use of the nso product to support any FBI investigation.”)

The advent of advanced spyware has transformed the world of espionage and surveillance. Bringing together a largely unregulated

industry with an invasive-by-design digital ecosystem in which smart-phones and other personal devices contain the most intimate details of people's lives, the new technology can track almost anyone, anywhere in the world. Governments have taken notice. For Israel, which approves export licenses for nso Group's Pegasus, the sale of spyware to foreign governments has brought new diplomatic clout in countries as disparate as India and Panama; a *New York Times* investigation found that nso deals helped Israeli Prime Minister Benjamin Netanyahu seal the Abraham Accords with Bahrain, Morocco, and the UAE. In turn, client states have used Pegasus against not only opposition groups, journalists, and nongovernmental organizations (NGOs) but also geopolitical rivals. In 2020 and 2021, the Citizen Lab discovered that several devices belonging to officials in the United Kingdom's Foreign Commonwealth and Development Office had been hacked with Pegasus, and that a client of nso Group in the UAE had used the spyware to infiltrate a device located at 10 Downing Street, the residence of the British prime minister. In November 2021, the tech giant Apple notified 11 staff members of the U.S. embassy in Uganda that their iPhones had been hacked with Pegasus.

In response to these revelations, spyware firms have generally denied responsibility for their clients' abuses or have declined to comment. In a statement to *The New Yorker* in April 2022, nso Group said, "We have repeatedly cooperated with governmental investigations, where credible allegations merit, and have learned from each of these findings and reports and improved the safeguards in our technologies." The Israeli company has also said that its technology is designed to help governments investigate crime and terrorism. But advanced spyware has now been implicated in human rights violations and interstate espionage in dozens of countries, and spyware companies have few legal obligations or incentives for public transparency or accountability. nso Group has not provided any specific information to counter the Citizen Lab's detailed evidence of abuses.

The consequences of the spyware revolution are profound. In countries with few resources, security forces can now pursue high-tech operations using off-the-shelf technology that is almost as easy to acquire as headphones from Amazon. Among democracies, the technology has become an irresistible tool that can be deployed with little oversight; in the last year alone, security agencies in at least four

With spyware,
governments
can stop protests
before they occur.

European countries—Greece, Hungary, Poland, and Spain—have been implicated in scandals in which state agencies have been accused of deploying spyware against journalists and political opposition figures. A global market for spyware also means that forms of surveillance and espionage that were once limited to a few major powers are now available to almost any country, and potentially to even more private firms. Left unregulated, the proliferation of this technology threatens to erode many of the institutions, processes, and values on which the liberal international order depends.

WE WILL SPY FOR YOU

The spyware revolution has emerged as a byproduct of a remarkable convergence of technological, social, and political developments over the past decade. Smartphones and other digital devices are vulnerable to surveillance because their applications often contain flaws and because they continually transmit data through insecure cellular and Internet networks. Although manufacturers of these technology platforms employ engineers to find and patch vulnerabilities, they tend to prioritize product development over security. By discovering and weaponizing “zero days”—software flaws that are unknown to their designers—spyware firms exploit the inherent insecurity of the digital consumer world.

But the extraordinary growth of the spyware market has also been driven by several broader trends. First, spyware takes advantage of a global digital culture that is shaped around always-on, always-connected smartphones. By hacking a personal device, spyware can provide its operators with a user’s entire pattern of life in real time. Second, spyware offers security agencies an elegant way to circumvent end-to-end encryption, which has become a growing barrier to government mass surveillance programs that depend on the collection of telecommunications and Internet data. By getting inside a user’s device, spyware allows its operators to read messages or listen to calls before they have been encrypted or after they have been decrypted; if the user can see it on the screen, so can the spyware. A third factor driving the industry’s growth has been the rise of digitally enabled protest movements. Popular upheavals such as the color revolutions in former Soviet states in the first decade of this century and the Arab Spring in 2010–11 took many autocrats by surprise, and the organizers often used phones to mobilize protesters. By offering an almost godlike way to get inside activist networks, spyware has opened

up a powerful new method for governments to monitor dissent and take steps to neutralize it before large protests occur.

Finally, the spyware industry has also been fueled by the growing privatization of national security. Just as governments have turned to private contractors for complicated or controversial military operations, they have discovered that they can outsource surveillance and espionage to better-equipped and less visible private actors. Like soldiers of fortune, advanced spyware companies tend to put revenues ahead of ethics, selling their products without regard to the politics of their clients—giving rise to the term “mercenary spyware”—and like military contractors, their dealings with government security agencies are often cloaked in secrecy to avoid public scrutiny. Moreover, just as military contractors have offered lucrative private-sector careers for veterans of military and intelligence agencies, spyware firms and government security services have been building similarly mutually beneficial partnerships, boosting the industry in the process. Many senior members of nso Group, for example, are veterans of Israeli intelligence, including the elite Military Intelligence Directorate.

Although lack of transparency has made the mercenary spyware industry difficult to measure, journalists have estimated it to be worth about \$12 billion per year. Before recent financial setbacks brought on by a growing number of lawsuits, nso Group was valued at \$2 billion, and there are other major players in the market. Many companies now produce sophisticated spyware, including Cytrox (founded in North Macedonia and now with operations in Hungary and Israel), Israel-based Cyberbit and Candiru, Italy-based Hacking Team (now defunct), and the Anglo-German Gamma Group. Each of these firms can hypothetically serve numerous clients. Governments that appear to have used Cytrox’s Predator spyware, for example, include Armenia, Egypt, Greece, Indonesia, Madagascar, and Serbia. In 2021, Mexico’s secretary of Security and Public Safety, Rosa Icela Rodríguez, said that previous Mexican administrations had signed multiple contracts with nso Group, totaling \$61 million, to buy Pegasus spyware, and as Mexican and international researchers have shown, the government has kept using Pegasus despite the present leadership’s public assurances that it would not. (In October 2022, Mexican President Andrés Manuel López Obrador denied the findings, stating that his administration was not using the spyware against journalists or political opponents.)

On the basis of such lucrative deals, spyware firms have enjoyed backing from major private equity funds, such as the San Francisco

firm Francisco Partners and the London-based Novalpina Capital, thus bolstering their resources. Francisco Partners, which had a controlling stake in NSO Group for five years, told Bloomberg News in 2021, “[We are] deeply committed to ethical business practices, and we evaluate all our investments through that lens.” Novalpina, which together with NSO’s founders acquired Francisco Partners’ stake in 2019, said it would bring the spyware firm “in full alignment with UN guiding principles on business and human rights,” but revelations of abuses of Pegasus have continued, and correspondence published by *The Guardian* in 2022 indicated that Novalpina sought to discredit NSO Group’s critics, including this author. (Lawyers for Novalpina told *The Guardian* that these were “tenuous and unsubstantiated allegations.”) After a dispute between Novalpina’s founding partners, the firm lost its controlling stake in NSO Group in 2021.

But the spyware industry also includes far less sophisticated firms in countries such as India, the Philippines, and Cyprus. As the surveillance equivalent of strip-mall phone repair shops, such outfits may lack the ability to identify zero days, but they can still accomplish objectives through simpler means. They may use credential phishing—using false pretenses, often via email or text message, to obtain a user’s digital passwords or other sensitive personal information—or they may simply purchase software vulnerabilities from other hackers on the black market. And these smaller firms may be more willing to undertake illegal operations on behalf of private clients because they are located outside the jurisdiction in which a victim resides or because enforcement is lax.

It is hard to overestimate the reach and power of the latest commercial spyware. In its most advanced forms, it can silently infiltrate any vulnerable device anywhere in the world. Take the zero-day, zero-click exploit that Citizen Lab researchers discovered in 2021 on a Pegasus-infected iPhone. Using the exploit, which researchers called ForcedEntry, a spyware operator can surreptitiously intercept texts and phone calls, including those encrypted by apps such as Signal or WhatsApp; turn on the user’s microphone and camera; track movements through a device’s GPS; and gather photos, notes, contacts, emails, and documents. The operator can do almost anything a user can do and more, including reconfigure the device’s security settings and acquire the digital tokens that are used to securely access cloud accounts so that surveillance on a target can continue even after the exploit has been removed from a device—all without the target’s awareness. After the Citizen Lab shared Pegasus’s ForcedEntry

with analysts at Apple and Google, Google's analysts described it as "one of the most technically sophisticated exploits we've ever seen," noting that it provided capabilities that were "previously thought to be accessible to only a handful of nation states."

SHOOTING THE MESSENGERS

Over the past decade, the rise of authoritarian regimes in many parts of the world has raised new questions about the durability of the liberal international order. As has been widely noted, many ruling elites have been able to slide toward authoritarianism by limiting or controlling political dissent, the media, the courts, and other institutions of civil society. Yet far less attention has been paid to the pervasive role of the mercenary spyware industry in this process. This neglect is partly the result of how little we know about spyware, including, in many cases, the identity of the specific government agencies that are using it. (Given the secretive nature of spyware transactions, it is far easier to identify victims than operators.) There is little doubt, however, that spyware has been used to systematically degrade liberal democratic practices and institutions.

One of the technology's most frequent uses has been to infiltrate opposition movements, particularly in the run-up to elections. Researchers have identified cases in which opposition figures have been targeted, not only in authoritarian states such as Saudi Arabia and the UAE but also in democratic countries such as India and Poland. Indeed, one of the most egregious cases arose in Spain, a parliamentary democracy and European Union member. Between 2017 and 2020, the Citizen Lab discovered, Pegasus was used to eavesdrop on a large cross section of Catalan civil society and government. The targets included every Catalan member of the European Parliament who supported independence for Catalonia, every Catalan president since 2010, and many members of Catalan legislative bodies, including multiple presidents of the Catalan parliament. Notably, some of the targeting took place amid sensitive negotiations between the Catalan and Spanish governments over the fate of Catalan independence supporters who were either imprisoned or in exile. After the findings drew international attention, Paz Esteban, the head of Spain's National Intelligence Center, acknowledged to Spanish lawmakers that spyware had been used against some Catalan politicians, and Esteban was subsequently fired. But it is still unclear which government agency was responsible, and which laws, if any, were used to justify such an extensive domestic spying operation.

In some countries, spyware has proved equally effective against journalists who are investigating those in power, with far-reaching consequences for both the targets and their sources. In 2015, several devices belonging to Mexican journalist Carmen Aristegui and a member of her family were sent Pegasus exploit links while she was investigating corruption involving then Mexican President Enrique Peña Nieto. There is no smoking gun that identifies the responsible party, though strong circumstantial evidence suggests a Mexican government agency. In 2021, a Hungarian journalist investigating corruption in President Viktor Orban's inner circle was hacked with Pegasus. (The Hungarian government subsequently acknowledged that it had purchased the technology.) And that same year, the cellphone of *New York Times* Middle East correspondent Ben Hubbard was infected with Pegasus while he was working on a book about Saudi Arabia's de facto leader, Crown Prince Mohammed bin Salman.

One Egyptian
opposition leader
was targeted by
two different
governments.

Almost as frequently, spyware has been used to undermine judicial officials and civil society organizations that are trying to hold governments to account. Take the case of Alberto Nisman, a well-known Argentine anticorruption prosecutor who was investigating an alleged criminal conspiracy by high-level Argentine officials. In January 2015, Nisman was found dead in suspicious circumstances—his death was later ruled a homicide—the day before he was to provide testimony to Congress implicating then president of Argentina Cristina Fernández de Kirchner and her foreign minister, Héctor Timerman, in a cover-up of alleged Iranian involvement in the 1994 bombing of a Jewish center in Buenos Aires. Later that year, the Citizen Lab documented how a South American hack-for-hire group had been contracted to target Nisman with spyware before his death, suggesting that someone in power was keen to peer into his investigations. In Mexico in 2017, a still unknown government agency or agencies used Pegasus spyware against human rights groups and international investigators that were tracking down potential government cover-ups of the notorious disappearance and gruesome murder of 43 students in Iguala, Mexico. Subsequent reports showed that the Mexican government had badly botched the investigations and that government

personnel were implicated in a cover-up—findings that might never have come to light without the efforts of civil society watchdogs.

Other common Pegasus targets are lawyers involved with prominent or politically sensitive cases. In most liberal democracies, attorney-client privilege is sacrosanct. Yet the Citizen Lab has identified a variety of cases in which spyware has been used to hack or target lawyers' devices. In 2015, the tactic was used against two lawyers in Mexico who were representing the families of Nadia Vera, a slain government critic and women's rights advocate. More recently, multiple lawyers representing prominent Catalans were targeted as part of the Spanish surveillance campaign. And in Poland, Pegasus spyware was used several times to hack the device of Roman Giertych, legal counsel to Donald Tusk, a former prime minister and the leader of the country's main opposition party. (In early 2022, Polish Deputy Prime Minister Jaroslaw Kaczynski publicly acknowledged that the government had bought Pegasus spyware but denied that it had been used against the Polish opposition.)

As the availability of spyware grows, private-sector clients are also getting in on the act. Consider the activities of BellTroX, an Indian hack-for-hire company responsible for extensive espionage on behalf of private clients worldwide. Between 2015 and 2017, someone used BellTroX's services against American nonprofits that were working to publicize revelations that the oil company ExxonMobil had hidden its research about climate change for decades. BellTroX has also been used to target U.S. organizations working on net neutrality, presumably at the behest of a different client or clients that were opposed to that reform. BellTroX also has a burgeoning business in the legal world; law firms in many countries have used the company's services to spy on opposing counsel. In April 2022, an Israeli private detective who acted as a broker for BellTroX pleaded guilty in U.S. court to wire fraud, conspiracy to commit hacking, and aggravated identity theft, but BellTroX's India-based operators have remained out of reach of the law. (Asked by Reuters in 2020 to respond to the findings, the company's founder, Sumit Gupta, denied any wrongdoing and declined to disclose his clients.)

NOWHERE TO HIDE

The proliferating use of spyware against political and civil society targets in advanced democracies is concerning enough. Even more threatening, however, may be the ways in which the technology has allowed authoritarian regimes to extend their repression far beyond

their own borders. In past decades, autocrats faced significant barriers to repressing citizens who had gone into exile. With spyware, however, an operator can get inside a political exile's entire network without setting foot inside the target's adopted country, and with very few of the risks and costs associated with conventional international espionage.

Examples of this new form of transnational repression are manifold. Beginning in 2016, Cyberbit was used to target Ethiopian dissidents, lawyers, students, and others in nearly 20 countries. In 2021, the phones of two prominent Egyptians—exiled opposition politician Ayman Nour, who has been living in Turkey, and the host of a popular news program (who has asked to remain anonymous for his own safety)—were hacked with Cytrox's Predator spyware. In fact, the phone of Nour, who is an outspoken critic of Egyptian President Abdel Fattah el-Sisi, was simultaneously infected with both Predator and NSO Group's Pegasus spyware, each apparently operated by separate government clients—Egypt in the case of Predator and either Saudi Arabia or the UAE in the case of Pegasus. In a statement to *Vice News*, Cyberbit said that the Israeli government oversees its technology and that “the intelligence and defense agencies that purchase these products are obligated to use them in accordance with the law.” In the Egyptian hacking case, Cytrox's CEO, Ivo Malinkovski, declined to comment; according to *Vice News*, he subsequently deleted references to Cytrox in his LinkedIn profile. (The governments of Egypt, Ethiopia, Saudi Arabia, and the UAE have declined to comment about the findings.)

Especially far-reaching has been the Saudi government's transnational spyware campaign. In 2018, a phone belonging to Ghanem al-Masarir, a Saudi dissident living in the United Kingdom, was hacked with Pegasus spyware. Coinciding with the infection of his device, al-Masarir was tracked down and physically assaulted by Saudi agents in London. Spyware may have also played a part in the notorious killing of the exiled Saudi journalist Jamal Khashoggi in the Saudi consulate in Turkey. In 2018, a phone owned by Omar Abdulaziz—a Saudi activist, Canadian permanent resident, and close confidant of Khashoggi—was hacked with Pegasus spyware. Abdulaziz and Khashoggi had been discussing their activism against the Saudi regime over what they mistakenly assumed were secure communications platforms. After Khashoggi's killing, forensic analysis revealed that the devices of several other people closest to Khashoggi, including his Egyptian wife and his Turkish fiancée, had also been infected. To what extent Khashoggi's

own phones were hacked is not known because his fiancée turned them over to Turkish authorities, who have withheld them from independent analysis, but his closest contacts were all under surveillance, providing Saudi agents with windows into Khashoggi's personal life, political activism, and movements in the months leading up to his murder. (The Saudi government has declined to comment on the revelations. In 2021, nso Group told *The Guardian*, "Our technology was not associated in any way with the heinous murder of Jamal Khashoggi.")

In fact, targeting regime critics abroad with spyware is only one of several ways the Saudi government has employed digital technology to neutralize dissent. For example, according to a U.S. federal indictment, a top adviser to Saudi Crown Prince Mohammed bin Salman paid a Twitter employee \$300,000 and provided other gifts in 2014 and 2015, apparently in exchange for spying on dissidents on the platform. The employee, who left Twitter in 2015, was convicted in U.S. court in 2022. When such tactics are used in combination with the type of highly intrusive surveillance that spyware represents, dissidents can come under extraordinary psychological pressure. Many victims of hacking have experienced debilitating shock knowing that their compromised devices have also put friends and associates at risk and that their every move is being watched. One female Saudi activist explained that being digitally targeted was a form of "psychological and emotional war" that caused her "endless fear and anxiety." By using spyware, autocrats and despots are thus able to clamp down on civil society networks well beyond their own borders even as they strengthen autocracy at home.

Despite a large and growing body of documentation about spyware abuses around the world, there are several reasons that the technology seems likely to become even more widespread. First, although much scrutiny of mercenary spyware firms has concerned their contracts with national government agencies, many firms market to more than one client in a given country, including local law enforcement. For example, in a fact-finding trip to Israel in the summer of 2022, officials for the European Parliament learned that nso Group has at least 22 clients in 12 European countries, suggesting that a significant number of these clients are subnational agencies. Such deals raise further questions about accountability, given that research has shown

One exploit
can turn on a
user's microphone
and camera.

that local law enforcement agencies are often more susceptible to abuses, such as racial profiling or corruption, and tend to have poor transparency and insufficient oversight.

Second, although some mercenary spyware firms such as NSO Group claim that they deal only with government clients, there is little to prevent them from selling their technology to private firms or corrupt individuals. Evidence suggests that some already do: in July 2022, Microsoft's Threat Intelligence Center issued a report on an Austria-based spyware and hack-for-hire firm called DSIRF that had targeted individuals in banks, law firms, and consultancies in several countries. Though Microsoft did not specify what type of clients hired DSIRF, the firm advertises "due diligence" services to businesses, implying that these hacking operations were undertaken on behalf of private clients. When Reuters asked DSIRF about the Microsoft report, the company declined to comment. Although it is illegal if done without a warrant, such private-sector hacking is less likely to be deterred when hackers' firms are located outside the jurisdiction in which the targeting occurs. As protections for privacy rights, freedom of the press, and independent courts, come increasingly under threat in many countries, it will likely become even easier for corrupt firms or oligarchs to deploy mercenary spyware without accountability.

Third, spyware has become a central component of a broader menu of surveillance tools, such as location tracking and biometric identification, used by many government security agencies. The more that spyware is incorporated into everyday intelligence gathering and policing, the harder it will be to rein it in. More ominously, spyware may soon acquire even more invasive capabilities by exploiting wearable applications, such as biomedical monitors, emotional detection technology, and Internet-connected neural networks currently in development. Already, many digital applications aim to drill deeper into the subliminal or the unconscious aspects of users' behavior and gather data on their health and physiology. It is no longer science fiction to envision spyware that might use covert access to these data about our biological or cognitive systems to monitor and even manipulate a victim's behavior and overall well-being.

RESTRAINING ORDERS

For nearly a decade, the mercenary spyware industry has been able to expand its reach across the globe largely without regulation or accountability. But that is a choice governments have made, not an

inevitable outcome that must simply be accepted. As civil society watchdogs and journalists have brought to light flagrant abuses, it has become more difficult for major spyware vendors and government clients to hide their operations. In Europe and the United States, committees have held hearings on spyware, and government agencies have begun to develop new policies to limit its use. Notably, the U.S. Commerce Department has placed nso Group, Candiru, and other hack-for-hire firms on an export restriction list, limiting their access to U.S. products and technology and sending a strong signal to potential investors that spyware companies are under growing scrutiny. Technology platforms have also taken action. Meta (the parent company of Facebook) and Apple have sued nso Group in U.S. courts, notified victims of spyware infections, and worked to support civil society watchdogs. Apple has also donated \$10 million to cybersurveillance research and has pledged to do likewise with any damages awarded from its lawsuit against nso Group.

But curbing the global spread of mercenary spyware will require a comprehensive approach. To begin with, companies need to devote far more resources to identifying and rooting out spyware and ensuring that their services are properly secured against exploitation. WhatsApp and Apple have already shown how to alert victims when spyware is detected and hold spyware vendors such as nso Group legally responsible for violations of their terms of service and other legal offenses. Whether through a shift in business culture, or more likely through stronger government regulations, technology platforms should also put more emphasis on security and scale back the relentless quest to vacuum up user data. In turn, the forensic investigations of the Citizen Lab, Amnesty International, journalists, and others will need to be broadened and supplemented by other organizations doing similar work, whether at NGOs, universities, or investigative news organizations. Digital forensic science and digital accountability should be recognized as a formal research discipline that can monitor spyware activity, assist victims and targets, and keep pressure on governments and corporations to be more transparent and accountable for their actions. For such a field to emerge, many years of public, private, and philanthropic support will be needed.

Ultimately, governments themselves will need to adopt a robust regulatory framework for spyware use. Regulating the industry will likely require the enactment of a complex set of rules that address various aspects of the spyware market. For example, domestic-based

spyware companies could be required to make regular public disclosures about their exports, and, in turn, government agencies could be required to report from whom and where they are importing spyware. Export rules need to be strengthened to prevent the sale of spyware to governments or other clients that are likely to use them in violation of international human rights law. Clear rules and standards of oversight for the use of spyware are also necessary. Specific legislation addressing the zero-day market will likely also be needed, although it will have to be carefully crafted so that legitimate security research is not hindered. Governments could also pass legislation giving victims of spyware the right to sue both foreign governments and spyware vendors for harms caused by espionage.

Such efforts could be reinforced at an international level through the development of a global spyware control regime. Military activities, for example, have long been subject to international oversight through such mechanisms as the UN's Register of Conventional Arms and the policies that have been put in place relating to standards for private military and security contractors or the banning of land mines. A similar process could lead to the international regulation of spyware, including requirements for transparency and reporting about its use. These existing models, however, suggest that success will require the buy-in of a significant number of countries, and more pressure is needed to persuade governments and world leaders that mercenary spyware poses a serious and growing threat to international security and the liberal international order.

No doubt, authoritarian governments and security agencies that currently benefit from spyware will seek to obstruct such regulation, but the growing risks to national security of an unregulated market may prompt a more sober assessment. In November 2022, Sir Jeremy Fleming, a top British intelligence official, warned that the proliferating use of mercenary spyware and "hackers for hire" by countries and malefactors "will increase the future threat to UK cybersecurity." Should the use of mercenary spyware continue to grow unchecked, the risks for democracy will become acute. If elites in any country can use this technology to neutralize legitimate political opposition on any point on earth, silence dissent through targeted espionage, undermine independent journalism, and erode public accountability with impunity, then the values on which the liberal international order is built may soon be no more secure than the passwords on our phones. 🌐

FW: [EXTERNAL] The Cybersecurity 202: A longtime DOJ cyber official gives an exclusive exit interview

From: "Mak, Hansen L. EOP/NCD" <(b) (6)>
To: "Dudley, Drenan E. EOP/NCD" <(b) (6)>
Date: Thu, 23 Feb 2023 08:59:37 -0500

FYSA on use of disruptive technology by DoJ and creation of a Strike Force. My assumption is that minimal to no additional funds are needed if they absorb within.

[Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force | OPA | Department of Justice](#)

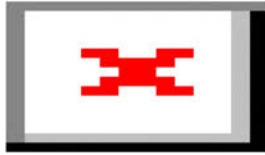
The strike force's work will focus on investigating and prosecuting criminal violations of export laws; enhancing administrative enforcement of U.S. export controls; fostering partnerships with the private sector; leveraging international partnerships to coordinate law enforcement actions and disruption strategies; utilizing advanced data analytics and all-source intelligence to develop and build investigations; conducting regular trainings for field offices; and strengthening connectivity between the strike force and the Intelligence Community.

In addition to the National Security Division and the Bureau of Industry and Security, this strike force will be comprised of officials from designated U.S. Attorneys' Offices throughout the country, the FBI and the Department of Homeland Security's Homeland Security Investigations (HSI).

From: The Washington Post <email@washingtonpost.com>
Sent: Thursday, February 23, 2023 7:18 AM
To: Mak, Hansen L. EOP/NCD <(b) (6)>
Subject: [EXTERNAL] The Cybersecurity 202: A longtime DOJ cyber official gives an exclusive exit interview



[View in browser](#)



By Tim Starks

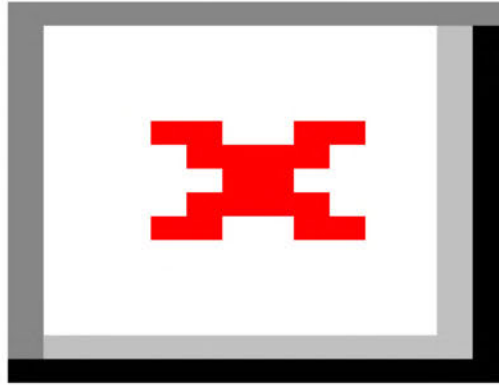
with research by Vanessa Montalbano

Welcome to The Cybersecurity 202! We'll have the day off from publishing Friday, so see you next on Monday.

Reading this online? *Sign up for The Cybersecurity 202 to get scoops and sharp analysis in your inbox each morning.*

Below: The European Commission bans TikTok on staffers' official devices, and states are crafting their own online privacy standards after a bipartisan bill failed in Congress last year. First:

Adam Hickey discusses his time working on cyber issues at DOJ, and what's next



Adam Hickey plans to join a law firm. (Carolyn Kaster/AP)

Adam Hickey, who has spent more than a decade at the Justice Department working on high-profile cyber cases, is leaving the department to go into the private sector. Hickey most recently served as deputy assistant attorney general at the Justice Department's National Security Division (NSD), where he supervised the office devoted to investigating and prosecuting nation-backed computer intrusions.

Hickey spoke with me on Wednesday about how the department has evolved its approach to cyber issues during his time there and some of the related areas he has focused on, like scrutinizing foreign companies investing in U.S. businesses. He also talked about challenges ahead for the department.

Hickey plans to join a law firm, which he declined to name. He began at the department in 2007 as a prosecutor in the Southern District of New York, then moving to the NSD in 2012 and taking his current role in 2016.

"When I came down here, my focus then was on building cases involving state actors conducting intrusions," Hickey said. "At the time, when we talked about cyber, one of the dominant topics was foreign governments hacking into systems and stealing either IP [intellectual property] or export control information. Now I think about how the cyber portfolio crosses across NSD."

A CHANGING DOJ

One of the key changes Hickey played a role in was the department increasingly naming who was responsible for major cyberattacks. “We live in a better world where we are transparent about what other actors or countries are doing, and what their employees are doing, and their proxies,” he said of an accomplishment that was “certainly not mine alone.”



- Leadership began treating cyber as not just an intelligence problem or diplomatic problem, recognizing the tools law enforcement can bring to bear to deter would-be attackers, Hickey said. Building cases demonstrates potential consequences even if the hackers are unlikely to see the inside of a jail cell, and it can scare off those who might be attracted to malicious hacking if they know they won't be able to leave their home country lest they be arrested, he said.
- Attributing attacks in charging documents also can aid the private sector, and stand to rally other allied countries, Hickey said — and all the better if other agencies and countries join in that attribution effort, as is increasingly common.

The U.S. first filed criminal charges against government-connected hackers in 2014, which made five Chinese military hackers the inaugural targets for their alleged widespread economic espionage. Some of the other major cases of Hickey's tenure, he said, have been the charging in 2017 of two alleged Russian spies and two cybercriminals whom they paid in the massive Yahoo hack; and the investigation of the hacks of Democratic organizations and officials in the lead-up to the 2016 elections.

Another notable shift, he said, was the department becoming “more comfortable using disruptive tools to either recoup gains or frustrate activities in the first place.” One example of that, Hickey said, is the operation last year to go into computers infected by a botnet — which takes over devices to use them for illicit aims, like spreading malware — without their owners authorizing it. By doing so, the department said, it was able to disable the grip a Russian government-controlled botnet called Cyclops Blink had on thousands of devices.^F

- The approach has raised privacy concerns, but Hickey said the department mitigates that by going to a court to get approval from a judge for a search warrant and eventually making affidavits public.
- The Cyclops Blink operation wouldn’t have been possible without a strong relationship with the private sector, as the department coordinated with WatchGuard Technologies, he said. The botnet had exploited a vulnerability in company firewalls.
- Despite the increased willingness to use them, Hickey called operations like the Cyclops Blink disruption a “tool of last resort.”

Hickey also touted stepped-up enforcement of the Foreign Agents Registration Act, which requires agents of foreign governments involved in political activities to disclose their affiliation. That includes the use of civil enforcement authority in 2019 for the first time since 1991, when a judge ordered a Florida broadcaster to register under the law for its work on behalf of a Russian state-owned media organization.

He counted as another accomplishment the growth of the Foreign Investment Review Section, which represents the department on the staff of the Committee on Foreign Investment in the United States (CFIUS). That multiagency committee reviews transactions involving foreign investments that could affect national security.

According to the New York Times, Hickey has been one of the government officials negotiating with TikTok on behalf of CFIUS in response to the national security concerns raised by Chinese ownership of the app. Hickey said he couldn’t comment on the status of the TikTok process.

LOOKING AHEAD

Historically, “we have tended to undervalue or underprice security, as consumers and as businesses,” he said. “But there’s obviously a trend toward regulation, and I don’t know how the federal government will ultimately tackle that.”

Another challenge moving forward is what Hickey considers to be a “blending of the threats.” Before, the department was focused on “card-carrying intelligence officers,” he said, but lately he’s been focused on criminals who are acting with impunity in nations that aren’t cracking down on them.



Ransomware gangs showed signs of having less success last year. But even if gains in the fight against ransomware are temporary, they’re still valuable, Hickey said.

“No one involved in law enforcement thinks we’re going to end crime,” he said. “You’re bailing water out of a boat that has a hole in the hull. But if you didn’t bail the water out, it would undoubtedly be worse.” That means taking the fight to the gangs, forcing them to retool, and arresting as many of them as possible, even if it’s a small number, he said.

The department hailed Hickey’s tenure at the National Security Division.

“During that time, NSD has had unprecedented success in countering nation-state cyberthreats, enforcing sanctions and export controls, combating foreign malign influence and mitigating risks from foreign investment — in no small part because of Adam’s vision and leadership,” said **Luis Rossello**, a spokesperson.

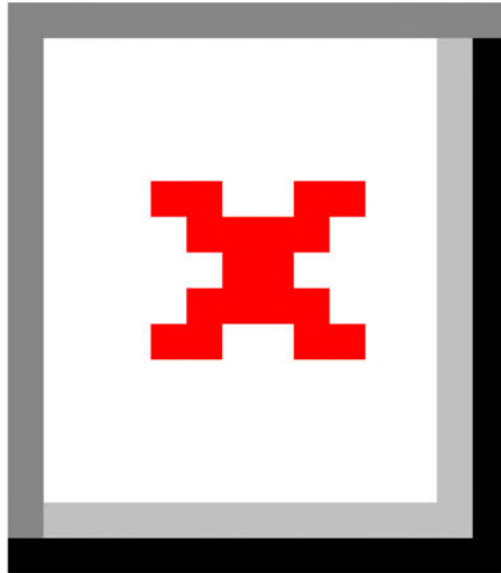
In Hickey’s absence, **Andrew Adams** will be serving as acting deputy assistant attorney general on an interim basis.

Hickey didn’t come into the department with a background in technology, but said he had an enthusiasm for national security, an interest in surveillance law and other “technocrat” leanings. Now he’s seeing more lawyers joining the department with computer science education and younger people who are “digital natives.” That can only help going forward, he said.

“I refer to it as a language that everyone uses everyday without being able to speak, and that’s kind of dangerous,” Hickey said, but “yeah, I’m optimistic.”

The keys

European Commission bans TikTok on staff phones



The European Commission's ban follows similar announcements in the United States and other countries. (Reuters/Yves Herman)

The European Commission banned its staff from using TikTok on work phones, following similar restrictions in the United States, [Emily Rauhala and Beatriz Ríos report](#). Staff members have been told that they have to remove TikTok from official devices, as well as personal phones that have work apps installed.

"The decision to restrict access for thousands of employees comes amid growing Western concern about Chinese technology, particularly links between tech companies and the Chinese government and the potential for data harvesting," Emily and Beatriz write. "In December, Congress banned the app from all federal devices. More than two dozen states have introduced similar bans. The commission's decision could lead to moves from other E.U. institutions."

TikTok has argued that it doesn't pose a security threat, and the company has launched a charm offensive to try to prove that it's not a national security threat.

Venture capital financing for cyber fell to \$18.5 billion in 2022

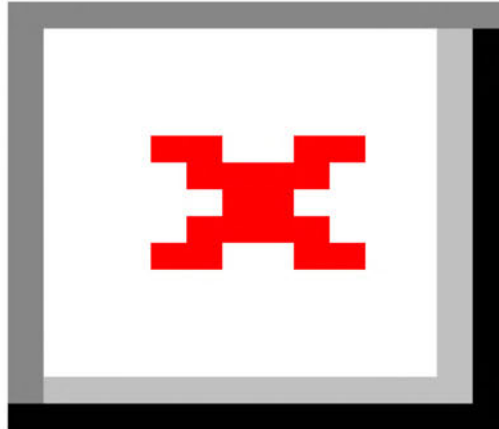
In the second half of 2022, venture capital investments for cybersecurity firms fell to \$18.5 billion from \$30.3 billion in 2021, according to the financial research firm Momentum Cyber, The Record's Jonathan Greig reports.

Still, experts said that 2022 marked the industry's highest year on record and that the unpredictable economy that prevailed over the last year due to Russia's invasion of Ukraine likely impacted how much firms would be willing to invest in publicly traded start-ups. They warned, however, that the threat from cyberattacks is accelerating.

"While cybersecurity venture investment slowed in the second half of the year, continued budget increases from security teams and ongoing cybersecurity and geopolitical risk gives us optimism about the long-term future of this industry," Momentum Cyber's executive chairman **Dave DeWalt** said.

"We live at a seminal time in cybersecurity history, with risk rising to levels greater than we have ever seen," DeWalt added.

States are taking on Americans' online privacy



Indiana lawmakers at the Indiana Statehouse in Indianapolis on Feb. 7. (Arleigh Rodgers/AP)

After a broad bipartisan federal privacy bill died in Congress last year, advocates are looking at state capitals to enact tough new restrictions on how Americans' personal data can be shared, create a data broker registry and establish new rights for Americans to delete data about themselves, Politico's Alfred Ng reports.

Already, politicians in Massachusetts and Illinois are proposing data privacy measures modeled after the failed bill while Democrats in Indiana are using it as inspiration to tighten legislation that has already been drafted. Four other states have also passed their own online privacy laws in the past two years — prompting tech companies to worry about a future national “patchwork” of hard-to-navigate data rules.

The new statehouse focus is meant to strengthen regulations in just enough places to force the tech industry into a de facto national standard, Ng writes. But a powerful industry-led campaign is already underway in several states, including Virginia and Utah, where weaker laws were enacted over the past two years.

The sector argues that a series of individual state privacy laws, including any that follow the proposed federal regulation, would create confusion for companies and citizens — and instead

of satisfying multiple systems, they are more likely to accommodate whatever the toughest standard is.

The American Data Privacy and Protection Act enjoyed broad bipartisan support on Capitol Hill and rare backing from both the tech industry and privacy advocates. But it was ultimately shot down by California Democrats, led by then-House Speaker Nancy Pelosi because of concerns that a national framework would weaken strong protections that the state has had since 2018.

Securing the ballot

Arizona's top prosecutor concealed records debunking election fraud claims

By Yvonne Wingett Sanchez and Isaac Stanley-Becker • [Read more »](#)

Global cyberspace

Ukraine suffered more data-wiping malware in 2022 than anywhere, ever

By Wired • [Read more »](#)

Putin silenced by Pro-Ukrainian hackers during DDoS attack on Russian media

By Cybernews • [Read more »](#)

Cyber insecurity

Cyberattack on food giant Dole temporarily shuts down North America production, company memo says

By CNN • [Read more »](#)

More vulnerabilities in industrial systems raise fresh concerns about critical infrastructure hacks

By CyberScoop • [Read more »](#)

NSA shares guidance on how to secure your home network

By Bleeping Computer • [Read more »](#)

Phone hackers use Florida man's password to steal \$65K from bank account

By Click Orlando • [Read more »](#)

New S1deload Stealer malware hijacks Youtube, Facebook accounts

By Bleeping Computer • [Read more »](#)

Ransomware prevention saw 'massive' improvement in 2022

By CRN • [Read more »](#)



Industry report

AT&T seeks to shed cybersecurity division

By Reuters • [Read more »](#)

Government scan

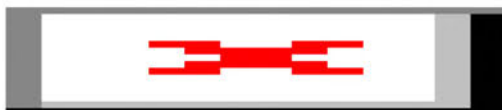
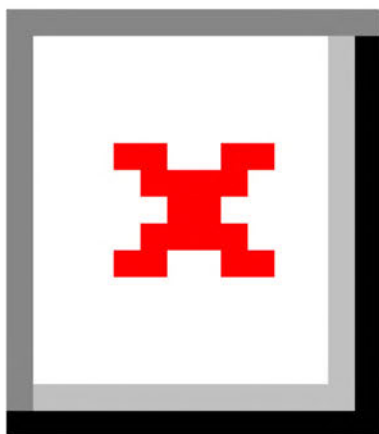
[The Energy Department's Puesh Kumar on grid hacking, Ukraine and Pipedream malware](#)

By CyberScoop • [Read more »](#)

Daybook

- The R Street Institute [holds a webinar](#) on the state of cybersecurity careers for Black professionals today at noon.
- Former U.S. national security adviser John Bolton Will [join The Washington Post](#) for a conversation about the war in Ukraine and rising tensions with China on Friday at 11 a.m.

Secure log off



Thanks for reading. See you next week.



[Manage my email newsletters and alerts](#) | [Unsubscribe from The Cybersecurity 202](#) | [Privacy Policy](#) | [Help](#)

You received this email because you signed up for The Cybersecurity 202 or because it is included in your subscription.

©2023 The Washington Post | 1301 K St NW, Washington DC 20071



Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
To: "Stupak, Philip M. EOP/NCD" (b) (6) >
Cc: sgarnault@garnault-associes.com
Date: Tue, 28 Feb 2023 17:19:01 -0500

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm? Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak, Philip M. EOP/NCD (b) (6) > a écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP Izard and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban. We would like to better understand the delegation's thoughts on the Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) as I understand that EU Member State cyber experts and ENISA are likely meeting in the near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Sent: Tuesday, February 28, 2023 8:04 AM
To: Stupak, Philip M. EOP/NCD (b) (6) >
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.

I am contacting you regarding the meeting.

MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passeport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver <pahouver@garnault-associes.com> a écrit :

Dear Philip,

Thank you very much!

I've just completed the form for every member of our delegation. Is it ok on your side?

Do not hesitate to tell me if you need additional information.

Please also find enclosed le list of the members of our delegation.

I remain at your entire disposal for any further information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this form: <https://events.whitehouse.gov/AppointmentRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Sent: Monday, February 27, 2023 2:22 PM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino, 35000 Rennes
+ 33 6 86 51 56 96 - pahouver@garnault-associes.com

Le 27 févr. 2023 à 13:59, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

Hello Sébastian,

Apologies for the delay—your email came as we departed for the Munich Security Conference and we have been sorting schedules on our return. Unfortunately, (Acting) National Cyber Director Kemba Walden is unavailable to meet with the delegation. Our Deputy National Cyber Director Neal Higgins is available on Thursday, March 2, between 10am-12pm if that window works for you. Does your schedule permit an hour-long meeting during that window on Thursday?

Philip Stupak

Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

Begin forwarded message:

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Date: February 14, 2023 at 4:01:51 AM EST
To: "Walden, Kemba E. EOP/NCD" <(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: [EXTERNAL] Meeting proposition - French CyberTaskForce
Delegation | February 27th to March 3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you during our stay in D.C.**

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation
3. **Mr Alexis Izard**, Member of Parliament, author of the information report "Investing for France 2030" for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President « Digital and Cyber » of Pays de la Loire Regional Council
6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
7. **Mr Bruno Charrat**, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you and I stay personally at your entire disposal, and for your team, for any additional information you may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault

Founder of CyberTaskForce and Paris Cyber Summit

President of Garnault & Associés

27, boulevard Solférino - F-35 000 Rennes

+33 6 80 71 60 56 - sgarnault@garnault-associes.com

[@SebGarnault](#) - [Profil LinkedIn](#)

Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
To: "Stupak, Philip M. EOP/NCD" (b) (6) >
Cc: sgarnault@garnault-associes.com
Date: Tue, 28 Feb 2023 18:13:12 -0500

Thank you. I've just informed Sebastien and he is personally calling the CISA. I keep you posted.

However, a meeting with you is still very interesting and key for all of us. We've made a mistake...

Le 28 févr. 2023 à 17:56, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

I believe all of our deputies are in planned Friday meetings so you would be stuck with me. Because of the issue we'll discuss, our windows are very tight the next two weeks but we wanted to ensure an opportunity to meet with you.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:47 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Thank you Philip for your fast answer.

We apologize, it is our mistake.. I am calling right now CISA to see what I can do. To make sure that we explore all possibilities, would be Friday morning available for you or not at all ? Sorry to ask...

Le 28 févr. 2023 à 17:39, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

Unfortunately, we have very little flexibility for a reason that I cannot discuss before Thursday. Should we still be able to meet on Thursday as planned then we will be able to brief you on that item and you will understand the lack of flexibility. Sorry!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director

Executive Office of the President

On Feb 28, 2023, at 5:19 PM, Pierre-Alexandre Houver <pahouver@garnault-associates.com> wrote:

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm? Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak, Philip M. EOP/NCD
<(b) (6)> a écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP Izard and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban. We would like to better understand the delegation's thoughts on the Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) as I understand that EU Member State cyber experts and ENISA are likely meeting in the near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Sent: Tuesday, February 28, 2023 8:04 AM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce
Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.

I am contacting you regarding the meeting.

MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver <pahouver@garnault-associes.com> a écrit :

Dear Philip,

Thank you very much!

I've just completed the form for every member of our delegation. Is it ok on your side?

Do not hesitate to tell me if you need additional information.

Please also find enclosed le list of the members of our delegation.

I remain at your entire disposal for any further information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this form: <https://events.whitehouse.gov/AppointmentRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associés.com>

Sent: Monday, February 27, 2023 2:22 PM

To: Stupak, Philip M. EOP/NCD (b) (6)

Cc: sgarnault@garnault-associés.com

Subject: Re: [EXTERNAL] Meeting proposition - French
CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino, 35000 Rennes
+ 33 6 86 51 56 96 - pahouver@garnault-associés.com

Le 27 févr. 2023 à 13:59, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

Hello Sébastien,

Apologies for the delay—your email came as we departed for the Munich Security Conference and we have been sorting schedules on our return. Unfortunately, (Acting) National Cyber Director Kemba Walden is unavailable to meet with the delegation. Our Deputy National Cyber Director Neal Higgins is available on Thursday, March 2, between 10am-12pm if that window works for you. Does your schedule permit an hour-long meeting during that window on Thursday?

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

Begin forwarded message:

From: Sébastien Garnault <sgarnault@garnault-associés.com>
Date: February 14, 2023 at 4:01:51 AM EST
To: "Walden, Kemba E. EOP/NCD"
<(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associés.com>
Subject: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you during our stay in D.C.**

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation
3. **Mr Alexis Izard**, Member of Parliament, author of the information report "Investing for France 2030" for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President « Digital and Cyber » of Pays de la Loire Regional Council
6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
7. **Mr Bruno Charrat**, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you and I stay personally at your entire disposal, and for your team, for any additional information you may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault

Founder of CyberTaskForce and Paris Cyber Summit
President of Garnault & Associés

27, boulevard Solférino - F-35 000 Rennes
+33 6 80 71 60 56 - sgarnault@garnault-associés.com
[@SebGarnault](#) - [Profil LinkedIn](#)

Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: "Stupak, Philip M. EOP/NCD" (b) (6) >
To: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Cc: sgarnault@garnault-associes.com
Date: Tue, 28 Feb 2023 17:39:19 -0500

Unfortunately, we have very little flexibility for a reason that I cannot discuss before Thursday. Should we still be able to meet on Thursday as planned then we will be able to brief you on that item and you will understand the lack of flexibility. Sorry!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:19 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm? Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak, Philip M. EOP/NCD (b) (6) > a écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP Izard and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban. We would like to better understand the delegation's thoughts on the Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) as I understand that EU Member State cyber experts and ENISA are likely meeting in the near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associates.com>
Sent: Tuesday, February 28, 2023 8:04 AM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: sgarnault@garnault-associates.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.
I am contacting you regarding the meeting.
MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passeport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver <pahouver@garnault-associes.com>
a écrit :

Dear Philip,

Thank you very much!

I've just completed the form for every member of our delegation. Is it ok on your side?

Do not hesitate to tell me if you need additional information.

Please also find enclosed the list of the members of our delegation.

I remain at your entire disposal for any further information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this

form: <https://events.whitehouse.gov/AppointmentRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Sent: Monday, February 27, 2023 2:22 PM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation
| February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino, 35000 Rennes
+ 33 6 86 51 56 96 - pahouwer@garnault-associes.com

Le 27 févr. 2023 à 13:59, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Hello Sébastien,

Apologies for the delay—your email came as we departed for the Munich Security Conference and we have been sorting schedules on our return. Unfortunately, (Acting) National Cyber Director Kemba Walden is unavailable to meet with the delegation. Our Deputy National Cyber Director Neal Higgins is available on Thursday, March 2, between 10am-12pm if that window works for you. Does your schedule permit an hour-long meeting during that window on Thursday?

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

Begin forwarded message:

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Date: February 14, 2023 at 4:01:51 AM EST
To: "Walden, Kemba E. EOP/NCD" <(b) (6)>
Cc: Pierre-Alexandre Houwer <pahouwer@garnault-associes.com>
Subject: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you during our stay in D.C.**

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and

awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation
3. **Mr Alexis Izard**, Member of Parliament, author of the information report "Investing for France 2030" for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President « Digital and Cyber » of Pays de la Loire Regional Council
6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
7. **Mr Bruno Charrat**, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you and I stay personally at your entire disposal, and for your team, for any additional information you may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault

Founder of CyberTaskForce and Paris Cyber Summit
President of Garnault & Associés

27, boulevard Solférino - F-35 000 Rennes
+33 6 80 71 60 56 - sgarnault@garnault-associés.com
[@SebGarnault](#) - [Profil LinkedIn](#)

Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
To: "Stupak, Philip M. EOP/NCD" (b) (6) >
Cc: sgarnault@garnault-associes.com
Date: Tue, 28 Feb 2023 17:46:49 -0500

Thank you Philip for your fast answer.

We apologize, it is our mistake.. I am calling right now CISA to see what I can do. To make sure that we explore all possibilities, would be Friday morning available for you or not at all ? Sorry to ask...

Le 28 févr. 2023 à 17:39, Stupak, Philip M. EOP/NCD (b) (6) > a écrit :

Unfortunately, we have very little flexibility for a reason that I cannot discuss before Thursday. Should we still be able to meet on Thursday as planned then we will be able to brief you on that item and you will understand the lack of flexibility. Sorry!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:19 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm? Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak, Philip M. EOP/NCD (b) (6) >
a écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP Izard and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban. We would like to better understand the delegation's thoughts on the Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) as I understand that EU Member State cyber experts and ENISA are likely meeting in the near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Sent: Tuesday, February 28, 2023 8:04 AM
To: Stupak, Philip M. EOP/NCD <(b) (6) >
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.

I am contacting you regarding the meeting.

MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passeport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver <pahouver@garnault-associes.com> a écrit :

Dear Philip,

Thank you very much!

I've just completed the form for every member of our delegation. Is it ok on your side?

Do not hesitate to tell me if you need additional information.

Please also find enclosed le list of the members of our delegation.

I remain at your entire disposal for any further information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this form: <https://events.whitehouse.gov/AppointmentRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associates.com>
Sent: Monday, February 27, 2023 2:22 PM
To: Stupak, Philip M. EOP/NCD (b) (6) >
Cc: sgarnault@garnault-associates.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino, 35000 Rennes
+ 33 6 86 51 56 96 - pahouver@garnault-associes.com

Le 27 févr. 2023 à 13:59, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

Hello Sébastien,

Apologies for the delay—your email came as we departed for the Munich Security Conference and we have been sorting schedules on our return. Unfortunately, (Acting) National Cyber Director Kemba Walden is unavailable to meet with the delegation. Our Deputy National Cyber Director Neal Higgins is available on Thursday, March 2, between 10am-12pm if that window works for you. Does your schedule permit an hour-long meeting during that window on Thursday?

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

Begin forwarded message:

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Date: February 14, 2023 at 4:01:51 AM EST
To: "Walden, Kemba E. EOP/NCD"
<(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you during our stay in D.C.**

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation
3. **Mr Alexis Izard**, Member of Parliament, author of the information report "Investing for France 2030" for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President « Digital and Cyber » of Pays de la Loire Regional Council
6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
7. **Mr Bruno Charrat**, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you and I stay personally at your entire disposal, and for your team, for any additional information you may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault

Founder of CyberTaskForce and Paris Cyber Summit
President of Garnault & Associés

27, boulevard Solférino - F-35 000 Rennes
+33 6 80 71 60 56 - sgarnault@garnault-associates.com
[@SebGarnault](#) - [Profil LinkedIn](#)

RE: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: "stupak, philip m. eop/ncd"
To: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Cc: sgarnault@garnault-associes.com
Date: Tue, 28 Feb 2023 10:03:19 -0500

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP Izard and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Sent: Tuesday, February 28, 2023 8:04 AM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.
I am contacting you regarding the meeting.
MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passeport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

(b) (6)

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver <pahouver@garnault-associes.com> a écrit :

Dear Philip,

Thank you very much!

I've just completed the form for every member of our delegation. Is it ok on your side?

Do not hesitate to tell me if you need additional information.

Please also find enclosed le list of the members of our delegation.

I remain at your entire disposal for any further information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this form: <https://events.whitehouse.gov/AppointmentRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associates.com>
Sent: Monday, February 27, 2023 2:22 PM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: sgarnault@garnault-associates.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino, 35000 Rennes
+ 33 6 86 51 56 96 - pahouver@garnault-associes.com

Le 27 févr. 2023 à 13:59, Stupak, Philip M. EOP/NCD (b) (6) > a écrit :

Hello Sébastien,

Apologies for the delay—your email came as we departed for the Munich Security Conference and we have been sorting schedules on our return. Unfortunately, (Acting) National Cyber Director Kemba Walden is unavailable to meet with the delegation. Our Deputy National Cyber Director Neal Higgins is available on Thursday, March 2, between 10am-12pm if that window works for you. Does your schedule permit an hour-long meeting during that window on Thursday?

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

Begin forwarded message:

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Date: February 14, 2023 at 4:01:51 AM EST
To: "Walden, Kemba E. EOP/NCD" <(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: [EXTERNAL] Meeting proposition - French CyberTaskForce
Delegation | February 27th to March 3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed

of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you during our stay in D.C.**

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation
3. **Mr Alexis Izard**, Member of Parliament, author of the information report "Investing for France 2030" for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President « Digital and Cyber » of Pays de la Loire Regional Council
6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
7. **Mr Bruno Charrat**, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you and I stay personally at your entire disposal, and for your team, for any additional information you may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault

Founder of CyberTaskForce and Paris Cyber Summit
President of Garnault & Associés

27, boulevard Solférino - F-35 000 Rennes
+33 6 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: Sébastien Garnault <sgarnault@garnault-associes.com>
To: "Stupak, Philip M. EOP/NCD" (b) (6) >
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Date: Wed, 01 Mar 2023 11:32:34 -0500

That is great.

I've contacted by my embassy who would like to invite you tonight at our cocktail. Please don't be surprise if you receive it today.

I wish you a wonderful day.
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 11:10, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

Wonderful, we are confirmed. I will meet you Friday, March 3, at 915am at the 17th Street and State Place entrance.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Sent: Wednesday, March 1, 2023 10:18 AM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

Thank you so much for the work ! It works perfectly and I confirm that we will all attend from 9:30 to 10:30.

Again, I apologise for the trouble.

With very best wishes,
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 10:12, Stupak, Philip M. EOP/NCD (b) (6) > a écrit :

We are able to accommodate Friday morning from 0930-1030. As feared, our deputies are all unavailable to meet but we can hold this meeting at the Assistant National Cyber Director level (the equivalent to an Agency Assistant Secretary). We are still confirming availabilities but we will likely have:

1. Nick Leiserson, ANCD for Cyber Policy & Programs
2. Drenan Dudley, ANCD for Budget Review & Assessment
3. Philip Stupak, (Acting) ANCD for International
4. Amanda Suarez, Senior Strategy & Research Advisor
5. Stephen Vina, Senior Advisor to the DNCD National Cybersecurity

Kindly let me know if that works for your delegation, and we will get the rooms and clearances moved over.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Sent: Tuesday, February 28, 2023 6:58 PM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation |
February 27th to March 3rd

Dear Philip,

I really appreciate what you are doing and thank you for your understanding. Let me know and I will make everything to make it the easiest for you.

Do not hesitate to use my number if needed (+33680716056).

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solferino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 18:51, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

Sébastien,

Let me work out some details with the team in the morning and see if we may make Friday morning work. I believe Neal Higgins will be otherwise unable to meet but I will hopefully be able to assemble a group of senior leaders from our Office.

I will revert early tomorrow.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director

Executive Office of the President

On Feb 28, 2023, at 6:40 PM, Sébastien Garnault <sgarnault@garnault-associes.com> wrote:

Director Stupak, dear Philip,

First of all, I would like to apologize deeply and formally. I feel very embarrassed for what is happening and I take back the lead from now on regarding our meeting.

I called CISA to see how the situation can be fixed. Unfortunately, we engaged too much work on strategic topics for both of our countries to cancel the workshop. This workshop involves many of your colleagues and it wouldn't be acceptable, and serious, to modify it.

However, I think key to meet you and make our bilateral discussion alive. I mean that if there is any opportunity to meet you on Friday morning, I would cancelled all we have, as it is not strategic for the delegation.

Again, it is very embarrassing and I hope you won't consider the situation as a lack of serious of the CyberTaskForce delegation.

What do you think ?

I stay personally available at anytime to sort it out.

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
+33 6 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 17:56, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

I believe all of our deputies are in planned Friday meetings so you would be stuck with me. Because of the issue we'll discuss, our windows are very tight the next two weeks but we wanted to ensure an opportunity to meet with you.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:47 PM, Pierre-Alexandre Houver

<pahouver@garnault-associes.com> wrote:

Thank you Philip for your fast answer.

We apologize, it is our mistake.. I am calling right now CISA to see what I can do. To make sure that we explore all possibilities, would be Friday morning available for you or not at all ? Sorry to ask...

Le 28 févr. 2023 à 17:39, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

Unfortunately, we have very little flexibility for a reason that I cannot discuss before Thursday. Should we still be able to meet on Thursday as planned then we will be able to brief you on that item and you will understand the lack of flexibility. Sorry!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:19 PM, Pierre-Alexandre Houver

<pahouver@garnault-associes.com> wrote:

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm? Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP IZARD and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban. We would like to better understand the delegation's thoughts on the Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) as I understand that EU Member State cyber experts and ENISA are likely meeting in the near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Sent: Tuesday, February 28, 2023 8:04 AM
To: Stupak, Philip M. EOP/NCD
<(b) (6)>
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French
CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.
I am contacting you regarding the meeting.
MP Alexis Izard has not put his middle name in the form. I
tried to refill the form but it appears I cannot do it as it has
already been submitted. I don't know if this can be
problematic? (I'm attaching to this email his passport).

Moreover, if possible of course, we would be more than
interested to talk about the TikTok ban from government
phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver
<pahouver@garnault-associes.com> a écrit :

Dear Philip,

Thank you very much!

I've just completed the form for every member of our delegation. Is it ok on your side?

Do not hesitate to tell me if you need additional information.

Please also find enclosed the list of the members of our delegation.

I remain at your entire disposal for any further information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36, Stupak, Philip M.
EOP/NCD <(b) (6)> a écrit
:

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this

form: <https://events.whitehouse.gov/AppointmentsRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Pierre-Alexandre Houver
<pahouver@garnault-associes.com>
Sent: Monday, February 27, 2023 2:22 PM
To: Stupak, Philip M. EOP/NCD
(b) (6) >
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver

Advisor to the president

27 boulevard de Solférino, 35000 Rennes
+ 33 6 86 51 56 96 - pahouver@garnault-associes.com

Le 27 févr. 2023 à 13:59, Stupak, Philip M.
EOP/NCD <(b) (6)> a écrit :

Hello Sébastian,

Apologies for the delay—your email came as we departed for the Munich Security Conference and we have been sorting schedules on our return. Unfortunately, (Acting) National Cyber Director Kemba Walden is unavailable to meet with the delegation. Our Deputy National Cyber Director Neal Higgins is available on Thursday, March 2, between 10am-12pm if that window works for you. Does your schedule permit an hour-long meeting during that window on Thursday?

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

Begin forwarded message:

From: Sébastien Garnault
<sgarnault@garnault-associes.com>
Date: February 14, 2023 at 4:01:51 AM
EST
To: "Walden, Kemba E. EOP/NCD"
<(b) (6)>
Cc: Pierre-Alexandre Houver
<pahouver@garnault-associes.com>
Subject: [EXTERNAL] Meeting
proposition - French CyberTaskForce
Delegation | February 27th to March
3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you during our stay in D.C.**

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation

3. **Mr Alexis Izard**, Member of Parliament, author of the information report “Investing for France 2030” for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President « Digital and Cyber » of Pays de la Loire Regional Council
6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
7. **Mr Bruno Charrat**, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you and I stay personally at your entire disposal, and for your team, for any additional information you may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault
Founder of CyberTaskForce and
Paris Cyber Summit
President of Garnault & Associés

27, boulevard Solférino - F-35 000
Rennes
+33 6 80 71 60 56
- sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: Sébastien Garnault <sgarnault@garnault-associes.com>
To: "Stupak, Philip M. EOP/NCD" (b) (6) >
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Date: Wed, 01 Mar 2023 10:17:42 -0500

Dear Philip,

Thank you so much for the work ! It works perfectly and I confirm that we will all attend from 9:30 to 10:30.

Again, I apologise for the trouble.

With very best wishes,
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 10:12, Stupak, Philip M. EOP/NCD (b) (6) > a écrit :

We are able to accommodate Friday morning from 0930-1030. As feared, our deputies are all unavailable to meet but we can hold this meeting at the Assistant National Cyber Director level (the equivalent to an Agency Assistant Secretary). We are still confirming availabilities but we will likely have:

1. Nick Leiserson, ANCD for Cyber Policy & Programs
2. Drenan Dudley, ANCD for Budget Review & Assessment
3. Philip Stupak, (Acting) ANCD for International
4. Amanda Suarez, Senior Strategy & Research Advisor
5. Stephen Vina, Senior Advisor to the DNCD National Cybersecurity

Kindly let me know if that works for your delegation, and we will get the rooms and clearances moved over.

Philip Stupak

Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Sébastien Garnault <sgarnault@garnault-associés.com>
Sent: Tuesday, February 28, 2023 6:58 PM
To: Stupak, Philip M. EOP/NCD (b) (6) >
Cc: Pierre-Alexandre Houver <pahouver@garnault-associés.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I really appreciate what you are doing and thank you for your understanding. Let me know and I will make everything to make it the easiest for you.

Do not hesitate to use my number if needed (+33680716056).

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associés.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 18:51, Stupak, Philip M. EOP/NCD (b) (6) > a écrit :

Sébastien,

Let me work out some details with the team in the morning and see if we may make Friday morning work. I believe Neal Higgins will be otherwise unable to meet but I will hopefully be able to assemble a group of senior leaders from our Office.

I will revert early tomorrow.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 6:40 PM, Sébastien Garnault <sgarnault@garnault-associés.com> wrote:

Director Stupak, dear Philip,

First of all, I would like to apologize deeply and formally. I feel very embarrassed for what is happening and I take back the lead from now on regarding our meeting.

I called CISA to see how the situation can be fixed. Unfortunately, we engaged too much work on strategic topics for both of our countries to cancel the workshop. This workshop involves many of your colleagues and it wouldn't be acceptable, and serious, to modify it.

However, I think key to meet you and make our bilateral discussion alive. I mean that if there is any opportunity to meet you on Friday morning, I would cancelled all we have, as it is not strategic for the delegation.

Again, it is very embarrassing and I hope you won't consider the situation as a lack of serious of the CyberTaskForce delegation.

What do you think ?

I stay personally available at anytime to sort it out.

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
+33 6 80 71 60 56 - sgarnault@garnault-associés.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 17:56, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

I believe all of our deputies are in planned Friday meetings so you would be stuck with me. Because of the issue we'll discuss, our windows are very tight the next two weeks but we wanted to ensure an opportunity to meet with you.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:47 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Thank you Philip for your fast answer.

We apologize, it is our mistake.. I am calling right now CISA to see what I can do. To make sure that we explore all possibilities, would be Friday morning available for you or not at all ? Sorry to ask...

Le 28 févr. 2023 à 17:39, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Unfortunately, we have very little flexibility for a reason that I cannot discuss before Thursday. Should we still be able to meet on Thursday as planned then we will be able to brief you on that item and you will understand the lack of flexibility. Sorry!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:19 PM, Pierre-Alexandre Houver
<pahouver@garnault-associes.com> wrote:

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm?
Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP Izard and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban. We would like to better understand the delegation's thoughts on the Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) as I understand that EU Member State cyber experts and ENISA are likely meeting in the near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
202-881-6385

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>

Sent: Tuesday, February 28, 2023 8:04 AM

To: Stupak, Philip M. EOP/NCD <(b) (6)>

Cc: sgarnault@garnault-associes.com

Subject: Re: [EXTERNAL] Meeting proposition - French
CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.

I am contacting you regarding the meeting.

MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passeport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver
<pahouver@garnault-associes.com> a écrit :

Dear Philip,

Thank you very much!

I've just completed the form for every member of our delegation. Is it ok on your side?

Do not hesitate to tell me if you need additional information.

Please also find enclosed le list of the members of our delegation.

I remain at your entire disposal for any further information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this

form:<https://events.whitehouse.gov/AppointmentRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and

"District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Sent: Monday, February 27, 2023 2:22 PM
To: Stupak, Philip M. EOP/NCD
<(b) (6)>
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino, 35000 Rennes
+ 33 6 86 51 56 96 - pahouver@garnault-associes.com

Le 27 févr. 2023 à 13:59, Stupak, Philip M. EOP/NCD
<(b) (6)> a écrit :

Hello Sébastien,

Apologies for the delay—your email came as we departed for the Munich Security Conference and we have been sorting schedules on our return. Unfortunately, (Acting) National Cyber Director Kemba Walden is unavailable to meet with the delegation. Our Deputy National Cyber Director Neal Higgins is available on Thursday, March 2, between 10am-12pm if that window works for you. Does your schedule permit an hour-long meeting during that window on Thursday?

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

Begin forwarded message:

From: Sébastien Garnault
<sgarnault@garnault-associes.com>
Date: February 14, 2023 at 4:01:51 AM EST
To: "Walden, Kemba E. EOP/NCD"
<(b) (6)>
Cc: Pierre-Alexandre Houver
<pahouver@garnault-associes.com>
Subject: [EXTERNAL] Meeting proposition
- French CyberTaskForce Delegation |
February 27th to March 3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you during our stay in D.C.**

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation
3. **Mr Alexis Izard**, Member of Parliament, author of the information report "Investing for France 2030" for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President « Digital and Cyber » of Pays de la Loire Regional Council
6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
7. **Mr Bruno Charrat**, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you and I stay personally at your entire disposal, and for your team, for any additional information you may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault

Founder of CyberTaskForce and Paris
Cyber Summit
President of Garnault & Associés

27, boulevard Solférino - F-35 000
Rennes

+33 6 80 71 60 56 - sgarnault@garnault-associés.com

[@SebGarnault](#) - [Profil LinkedIn](#)

Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: "Stupak, Philip M. EOP/NCD" <(b) (6)>
To: Sébastien Garnault <sgarnault@garnault-associes.com>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Date: Thu, 02 Mar 2023 09:11:42 -0500

Good news, the embargo has been lifted and I can formally share the strategy with you and your delegation. I enjoyed last night and look forward to tomorrow's discussion.

FACT SHEET

<https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>

NATIONAL CYBERSECURITY STRATEGY

<https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Mar 1, 2023, at 11:33 AM, Sébastien Garnault <sgarnault@garnault-associes.com> wrote:

That is great.

I've contacted by my embassy who would like to invite you tonight at our cocktail. Please don't be surprised if you receive it today.

I wish you a wonderful day.
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 11:10, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

Wonderful, we are confirmed. I will meet you Friday, March 3, at 915am at the 17th Street and State Place entrance.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Sent: Wednesday, March 1, 2023 10:18 AM
To: Stupak, Philip M. EOP/NCD (b) (6) >
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

Thank you so much for the work ! It works perfectly and I confirm that we will all attend from 9:30 to 10:30.

Again, I apologise for the trouble.

With very best wishes,
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solferino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 10:12, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

We are able to accommodate Friday morning from 0930-1030. As feared, our deputies are all unavailable to meet but we can hold this meeting at the Assistant National Cyber Director level (the equivalent to an Agency Assistant Secretary). We are still confirming availabilities but we will likely have:

1. Nick Leiserson, ANCD for Cyber Policy & Programs
2. Drenan Dudley, ANCD for Budget Review & Assessment
3. Philip Stupak, (Acting) ANCD for International
4. Amanda Suarez, Senior Strategy & Research Advisor
5. Stephen Vina, Senior Advisor to the DNCD National Cybersecurity

Kindly let me know if that works for your delegation, and we will get the rooms and clearances moved over.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
202-881-6385

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Sent: Tuesday, February 28, 2023 6:58 PM
To: Stupak, Philip M. EOP/NCD (b) (6)
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I really appreciate what you are doing and thank you for your understanding. Let me know and I will make everything to make it the easiest for you.

Do not hesitate to use my number if needed (+33680716056).

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-
Sent from my phone

Le 28 févr. 2023 à 18:51, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Sébastien,

Let me work out some details with the team in the morning and see if we may make Friday morning work. I believe Neal Higgins will be otherwise unable to meet but I will hopefully be able to assemble a group of senior leaders from our Office.

I will revert early tomorrow.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 6:40 PM, Sébastien Garnault <sgarnault@garnault-associés.com> wrote:

Director Stupak, dear Philip,

First of all, I would like to apologize deeply and formally. I feel very embarrassed for what is happening and I take back the lead from now on regarding our meeting.

I called CISA to see how the situation can be fixed. Unfortunately, we engaged too much work on strategic topics for both of our countries to cancel the workshop. This workshop involves many of your colleagues and it wouldn't be acceptable, and serious, to modify it.

However, I think key to meet you and make our bilateral discussion alive. I mean that if there is any opportunity to meet you on Friday morning, I would cancelled all we have, as it is not strategic for the delegation.

Again, it is very embarrassing and I hope you won't consider the situation as a lack of serious of the CyberTaskForce delegation.

What do you think ?

I stay personally available at anytime to sort it out.

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
+33 6 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 17:56, Stupak, Philip M. EOP/NCD

(b) (6) a écrit :

I believe all of our deputies are in planned Friday meetings so you would be stuck with me. Because of the issue we'll discuss, our windows are very tight the next two weeks but we wanted to ensure an opportunity to meet with you.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:47 PM, Pierre-Alexandre Houver
<pahouver@garnault-associes.com> wrote:

Thank you Philip for your fast answer.

We apologize, it is our mistake.. I am calling right now CISA to see what I can do. To make sure that we explore all possibilities, would be Friday morning available for you or not at all ? Sorry to ask...

Le 28 févr. 2023 à 17:39, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

Unfortunately, we have very little flexibility for a reason that I cannot discuss before Thursday. Should we still be able to meet on Thursday as planned then we will be able to brief you on that item and you will understand the lack of flexibility. Sorry!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:19 PM, Pierre-Alexandre Houver
<pahouver@garnault-associes.com> wrote:

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm? Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP Izard and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban. We would like to better understand the delegation's thoughts on the Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) as I understand that EU Member State cyber experts and ENISA are likely meeting in the near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>

Sent: Tuesday, February 28, 2023 8:04 AM

To: Stupak, Philip M. EOP/NCD

(b) (6)

Cc: sgarnault@garnault-associes.com

Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.

I am contacting you regarding the meeting.

MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passeport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver
<pahouver@garnault-associés.com> a écrit :

Dear Philip,

Thank you very much!

I've just completed the form for every member of
our delegation. Is it ok on your side?

Do not hesitate to tell me if you need additional
information.

Please also find enclosed the list of the members of
our delegation.

I remain at your entire disposal for any further
information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36, Stupak, Philip M.
EOP/NCD <(b) (6)> a
écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this
form:<https://events.whitehouse.gov/AppointmentRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
202-881-6385

From: Pierre-Alexandre Houver
<pahouver@garnault-associes.com>
Sent: Monday, February 27, 2023 2:22 PM
To: Stupak, Philip M. EOP/NCD
(b) (6) >
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting
proposition - French CyberTaskForce
Delegation | February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino, 35000 Rennes

+ 33 6 86 51 56 96 - pahouver@garnault-associes.com

Le 27 févr. 2023 à 13:59, Stupak, Philip M.
EOP/NCD (b) (6) > a
écrit :

Hello Sébastien,

Apologies for the delay—your email came as we departed for the Munich Security Conference and we have been sorting schedules on our return. Unfortunately, (Acting) National Cyber Director Kemba Walden is unavailable to meet with the delegation. Our Deputy National Cyber Director Neal Higgins is available on Thursday, March 2, between 10am-12pm if that window works for you. Does your schedule permit an hour-long meeting during that window on Thursday?

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President
(b) (6)

Begin forwarded message:

From: Sébastien Garnault
<sgarnault@garnault-associes.com>
Date: February 14, 2023 at 4:01:51 AM EST
To: "Walden, Kemba E. EOP/NCD"
<(b) (6)>
Cc: Pierre-Alexandre Houver
<pahouver@garnault-associes.com>
Subject: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you during our stay in D.C.**

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation
3. **Mr Alexis Izard**, Member of Parliament, author of the information report "Investing for France 2030" for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President

- « Digital and Cyber » of Pays de la Loire Regional Council
6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
 7. **Mr Bruno Charrat**, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
 8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
 9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you and I stay personally at your entire disposal, and for your team, for any additional information you may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault
Founder of CyberTaskForce and
Paris Cyber Summit
President of Garnault & Associés

27, boulevard Solférino - F-35
000 Rennes
+33 6 80 71 60 56
- sgarnault@garnault-associés.com
[@SebGarnault](#) - [Profil LinkedIn](#)

Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
To: "Stupak, Philip M. EOP/NCD" <(b) (6)>
Date: Thu, 02 Mar 2023 13:41:19 -0500

Perfect!
Thank you very much!

Le 2 mars 2023 à 13:11, Stupak, Philip M. EOP/NCD <(b) (6)> a écrit :

Yes, everyone cleared through background checks. Please have the delegation bring their passports tomorrow. Thanks!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Mar 2, 2023, at 1:08 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Just a quick question: is everything in order regarding the accreditations for tomorrow morning?

Thanks again!

Pierre-Alexandre

Le 2 mars 2023 à 13:04, Pierre-Alexandre Houver <pahouver@garnault-associes.com> a écrit :

Thank you very much for this Philip!

Pierre-Alexandre

Le 2 mars 2023 à 09:11, Stupak, Philip M. EOP/NCD
<(b) (6)> a écrit :

Good news, the embargo has been lifted and I can formally share the strategy with you and your delegation. I enjoyed last night and look forward to tomorrow's discussion.

FACT SHEET

<https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>

NATIONAL CYBERSECURITY STRATEGY

<https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Mar 1, 2023, at 11:33 AM, Sébastien Garnault <sgarnault@garnault-associés.com> wrote:

That is great.

I've contacted by my embassy who would like to invite you tonight at our cocktail. Please don't be surprise if you receive it today.

I wish you a wonderful day.
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associés.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 11:10, Stupak, Philip M. EOP/NCD
<(b) (6)> a écrit :

Wonderful, we are confirmed. I will meet you Friday, March 3, at 915am
at the 17th Street and State Place entrance.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Sent: Wednesday, March 1, 2023 10:18 AM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce
Delegation | February 27th to March 3rd

Dear Philip,

Thank you so much for the work ! It works perfectly and I confirm that we will all attend from 9:30 to 10:30.

Again, I apologise for the trouble.

With very best wishes,
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 10:12, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

We are able to accommodate Friday morning from 0930-1030. As feared, our deputies are all unavailable to meet but we can hold this meeting at the Assistant National Cyber Director level (the equivalent to an Agency Assistant Secretary). We are still confirming availabilities but we will likely have:

1. Nick Leiserson, ANCD for Cyber Policy & Programs
2. Drenan Dudley, ANCD for Budget Review & Assessment

3. Philip Stupak, (Acting) ANCD for International
4. Amanda Suarez, Senior Strategy & Research Advisor
5. Stephen Vina, Senior Advisor to the DNCD National Cybersecurity

Kindly let me know if that works for your delegation, and we will get the rooms and clearances moved over.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Sent: Tuesday, February 28, 2023 6:58 PM
To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I really appreciate what you are doing and thank you for your understanding. Let me know and I will make everything to make it the easiest for you.

Do not hesitate to use my number if needed (+33680716056).

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 18:51, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

Sébastien,

Let me work out some details with the team in the morning and see if we may make Friday morning work. I believe Neal Higgins will be otherwise unable to meet but I will hopefully be able to assemble a group of senior leaders from our Office.

I will revert early tomorrow.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 6:40 PM, Sébastien Garnault
<sgarnault@garnault-associes.com> wrote:

Director Stupak, dear Philip,

First of all, I would like to apologize deeply and formally. I feel very embarrassed for what is happening and I take back the lead from now on regarding our meeting.

I called CISA to see how the situation can be fixed. Unfortunately, we engaged too much work on strategic topics for both of our countries to cancel the workshop. This workshop involves many of your colleagues and it wouldn't be acceptable, and serious, to modify it.

However, I think key to meet you and make our bilateral discussion alive. I mean that if there is any opportunity to meet you on Friday morning, I would cancelled all we have, as it is not strategic for the delegation.

Again, it is very embarrassing and I hope you won't consider the situation as a lack of serious of the CyberTaskForce delegation.

What do you think ?

I stay personally available at anytime to sort it out.

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
+33 6 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 17:56, Stupak, Philip M. EOP/NCD

<(b) (6)> a écrit :

I believe all of our deputies are in planned Friday meetings so you would be stuck with me. Because of the issue we'll discuss, our windows are very tight the next two weeks but we wanted to ensure an opportunity to meet with you.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:47 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Thank you Philip for your fast answer.

We apologize, it is our mistake.. I am calling right now CISA to see what I can do. To make sure that we explore all possibilities, would be Friday morning available for you or not at all ? Sorry to ask...

Le 28 févr. 2023 à 17:39, Stupak, Philip M.
EOP/NCD <(b) (6)> a
écrit :

Unfortunately, we have very little flexibility for a reason that I cannot discuss before Thursday. Should we still be able to meet on Thursday as planned then we will be able to brief you on that item and you will understand the lack of flexibility. Sorry!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:19 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm? Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak,
Philip M. EOP/NCD

(b) (6) > a
écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted
MP Izard and reentered his
information based on the shared
passport. He should be good to
enter. I have also submitted all the
guests to clearance, and will alert
you if any issues arise with entered
information.

I can certainly cover the TikTok Ban.
We would like to better understand
the delegation's thoughts on the
Proposed Cybersecurity
Certification Scheme for Cloud
Services (EUCS) as I understand that
EU Member State cyber experts
and ENISA are likely meeting in the
near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber
Director
Executive Office of the President
(b) (6)

From: Pierre-Alexandre Houver
<[pahouver@gamault-
associates.com](mailto:pahouver@gamault-associates.com)>

Sent: Tuesday, February 28, 2023

8:04 AM

To: Stupak, Philip M. EOP/NCD

<(b) (6)>

Cc: sgarnault@garnault-associes.com

Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.

I am contacting you regarding the meeting.

MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passeport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13,
Pierre-Alexandre Houver
<[pahouver@garnault-
associes.com](mailto:pahouver@garnault-associes.com)> a écrit :

Dear Philip,

Thank you very much!
I've just completed the form
for every member of our
delegation. Is it ok on your
side?
Do not hesitate to tell me if
you need additional
information.
Please also find enclosed le list
of the members of our
delegation.

I remain at your entire disposal
for any further information you
may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DEL
EGATION.pdf>

Le 27 févr. 2023 à 14:36,
Stupak, Philip M.
EOP/NCD

<(b) (6)>
> a écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this form:<https://events.whitehouse.gov/AppointmentRsvpForm?rid=PWMB7M6MR3>

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks

are only required if you
are not vaccinated.

Given the tight turn
around, please ask your
delegation to complete
the form as soon as
possible, but no later than
tomorrow at noon ET.

Please reach out with any
questions.

Philip Stupak
Director Federal
Cybersecurity
Office of the National
Cyber Director
Executive Office of the
President

(b) (6)

From: Pierre-Alexandre
Houver

<[pahouver@garnault-
associates.com](mailto:pahouver@garnault-associates.com)>

Sent: Monday, February
27, 2023 2:22 PM

To: Stupak, Philip M.
EOP/NCD

(b) (6)

>

Cc: [sgarnault@garnault-
associates.com](mailto:sgarnault@garnault-associates.com)

Subject: Re: [EXTERNAL]
Meeting proposition -
French CyberTaskForce
Delegation | February
27th to March 3rd

Dear Philip,

Thank you very much for
your answer! We would
be very honored and
happy to meet with
Deputy National Cyber
Director Neal Higgins.

Thursday, March 2nd from
10 am to 11 am would
work perfectly for our
delegation.

I suppose that you may
need personal data for
access. Would you need
IDs number or any
information in order to
plan accesses?

Also, would it be possible
too to confirm the
location in order to plan
transports on our side?

Again, thank you very
much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino,
35000 Rennes
+ 33 6 86 51 56
96 - [pahouver@gamault-
associates.com](mailto:pahouver@gamault-associates.com)

Le 27 févr. 2023 à 13:59,
Stupak, Philip M.
EOP/NCD

(b) (6)
[REDACTED] a écrit :

Hello Sébastian,

Apologies for the
delay—your email
came as we departed
for the Munich

Security Conference
and we have been
sorting schedules on
our return.
Unfortunately,
(Acting) National
Cyber Director Kemba
Walden is unavailable
to meet with the
delegation. Our
Deputy National
Cyber Director Neal
Higgins is available on
Thursday, March 2,
between 10am-12pm
if that window works
for you. Does your
schedule permit an
hour-long meeting
during that window
on Thursday?

Philip Stupak
Director Federal
Cybersecurity
Office of the National
Cyber Director
Executive Office of
the President
202-881-6385

Begin forwarded
message:

From: Sébastien
Garnault
<sgarnault@garnault-associates.com>
Date: February
14, 2023 at
4:01:51 AM EST
To: "Walden,
Kemba E.
EOP/NCD"
<(b) (6)>
Cc: Pierre-

Alexandre
Houver
<pahouver@garnault-associes.com>
Subject: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Kemba,

I hope this mail will find you well.

I am writing this email following a discussion with **Mr Vincent Voci**, Vice-President at the US Chamber of Commerce. As president of the French CyberTaskForce, we are currently planning to come as a parliamentary delegation to Washington D.C. from February 27th to March 3rd. Composed of French Members of Parliaments, Civil servants and private sector decision-makers, we are coming to the US to meet our colleagues and counterparts involved in technologies, cyber and space.

In this context, we would be particularly honored to meet you for an exchange of views focused on Cyberdefense. **We would be very honored to meeting you**

during our stay in D.C.

As you know, cyber-attacks target large, small and critical organizations. However, addressing these threats become more and more complex for them as skills, materials and awareness are lacking. Therefore, we would be more than interested to have a 1 hour meeting with you to have a discussion on how US and France tackle these challenges and are working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the

French
Cyber
Task
Force,
founder
of Paris
Cyber
Summit
- Co-
head of
Delegati
on

3. **Mr
Alexis
Izard,**
Member
of
Parliam
ent,
author
of the
informat
ion
report
“Investi
ng for
France
2030”
for the
Finance
program
ming
Law for
2023

4. **Mr
Robin
Reda,**
Member
of
Parliam
ent,
member
of the
committ
ee for
Finance

5. **Ms
Consta
nce
Nebbul
a,** Vice-
Presiden
t
« Digita
l and
Cyber »
of Pays
de la
Loire R
egional
Council

6. **Mr Florent Kirchner**, Head of the French national cybersecurity strategy - Prime minister
7. **Mr Bruno Charra**t, Deputy Director of Technological Research at the CEA - Atomic Energy Commission, representative of the Alliance for Digital Trust (French cybersecurity professional association)
8. **Mr Pierre-Alexandre Houver**, Advisor at Garnault & Associés
9. **Mr Baptiste Robert**, CEO at Predicta Lab

I warmly thank you
and I stay personally
at your entire
disposal, and for your
team, for any
additional
information you may
need.

With best wishes,
Sébastien Garnault

--

**Sébastien
Garnault**
Founder of
CyberTaskForc
e and Paris
Cyber Summit
President of
Garnault &
Associés

27, boulevard
Solférino - F-35
000 Rennes
+33 6 80 71 60
56
- [sgarnault@gar
nault-
associés.com](mailto:sgarnault@garnault-associés.com)
[@SebGarnault](#) -
[Profil LinkedIn](#)

Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

From: "Stupak, Philip M. EOP/NCD" <(b) (6)>
To: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Cc: Sébastien Garnault <sgarnault@garnault-associes.com>
Date: Thu, 02 Mar 2023 13:11:36 -0500

Yes, everyone cleared through background checks. Please have the delegation bring their passports tomorrow. Thanks!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Mar 2, 2023, at 1:08 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Just a quick question: is everything in order regarding the accreditations for tomorrow morning?

Thanks again!

Pierre-Alexandre

Le 2 mars 2023 à 13:04, Pierre-Alexandre Houver <pahouver@garnault-associes.com> a écrit :

Thank you very much for this Philip!

Pierre-Alexandre

Le 2 mars 2023 à 09:11, Stupak, Philip M. EOP/NCD (b) (6) > a écrit :

Good news, the embargo has been lifted and I can formally share the strategy with you and your delegation. I enjoyed last night and look forward to tomorrow's discussion.

FACT SHEET

<https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>

NATIONAL CYBERSECURITY STRATEGY

<https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Mar 1, 2023, at 11:33 AM, Sébastien Garnault <sgarnault@garnault-associes.com> wrote:

That is great.

I've contacted by my embassy who would like to invite you tonight at our cocktail.
Please don't be surprise if you receive it today.

I wish you a wonderful day.
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 11:10, Stupak, Philip M. EOP/NCD
<(b) (6)> a écrit :

Wonderful, we are confirmed. I will meet you Friday, March 3, at 915am at
the 17th Street and State Place entrance.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Sent: Wednesday, March 1, 2023 10:18 AM

To: Stupak, Philip M. EOP/NCD <(b) (6)>
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce
Delegation | February 27th to March 3rd

Dear Philip,

Thank you so much for the work ! It works perfectly and I confirm that we will all attend from 9:30 to 10:30.

Again, I apologise for the trouble.

With very best wishes,
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 1 mars 2023 à 10:12, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

We are able to accommodate Friday morning from 0930-1030. As feared, our deputies are all unavailable to meet but we can hold this meeting at the Assistant National Cyber Director level (the equivalent to an Agency Assistant Secretary). We are still confirming availabilities but we will likely have:

1. Nick Leiserson, ANCD for Cyber Policy & Programs
2. Drenan Dudley, ANCD for Budget Review & Assessment
3. Philip Stupak, (Acting) ANCD for International
4. Amanda Suarez, Senior Strategy & Research Advisor
5. Stephen Vina, Senior Advisor to the DNCD National Cybersecurity

Kindly let me know if that works for your delegation, and we will get the rooms and clearances moved over.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Sébastien Garnault <sgarnault@garnault-associes.com>
Sent: Tuesday, February 28, 2023 6:58 PM
To: Stupak, Philip M. EOP/NCD (b) (6) >
Cc: Pierre-Alexandre Houver <pahouver@garnault-associes.com>
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce
Delegation | February 27th to March 3rd

Dear Philip,

I really appreciate what you are doing and thank you for your understanding. Let me know and I will make everything to make it the easiest for you.

Do not hesitate to use my number if needed (+33680716056).

With best wishes,
Sébastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce
Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
06 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 18:51, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

Sébastien,

Let me work out some details with the team in the morning and see if we may make Friday morning work. I believe Neal Higgins will be

otherwise unable to meet but I will hopefully be able to assemble a group of senior leaders from our Office.

I will revert early tomorrow.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 6:40 PM, Sébastien Garnault
<sgarnault@garnault-associes.com> wrote:

Director Stupak, dear Philip,

First of all, I would like to apologize deeply and formally. I feel very embarrassed for what is happening and I take back the lead from now on regarding our meeting.

I called CISA to see how the situation can be fixed. Unfortunately, we engaged too much work on strategic topics for both of our countries to cancel the workshop. This workshop involves many of your colleagues and it wouldn't be acceptable, and serious, to modify it.

However, I think key to meet you and make our bilateral discussion alive. I mean that if there is any opportunity to meet you on Friday morning, I would cancelled all we have, as it is not strategic for the delegation.

Again, it is very embarrassing and I hope you won't consider the situation as a lack of serious of the CyberTaskForce delegation.

What do you think ?

I stay personally available at anytime to sort it out.

With best wishes,
Sebastien

--

Sébastien Garnault
Fondateur de la CyberTaskForce

Président de Garnault & Associés

27, boulevard Solférino - Rennes (35000)
+33 6 80 71 60 56 - sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)

-

Sent from my phone

Le 28 févr. 2023 à 17:56, Stupak, Philip M. EOP/NCD

(b) (6) > a écrit :

I believe all of our deputies are in planned Friday meetings so you would be stuck with me. Because of the issue we'll discuss, our windows are very tight the next two weeks but we wanted to ensure an opportunity to meet with you.

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:47 PM, Pierre-Alexandre Houver
<pahouver@garnault-associes.com> wrote:

Thank you Philip for your fast answer.

We apologize, it is our mistake.. I am calling right now CISA to see what I can do. To make sure that we explore all possibilities, would be Friday morning available for you or not at all ? Sorry to ask...

Le 28 févr. 2023 à 17:39, Stupak, Philip M.

EOP/NCD <(b) (6)> a écrit :

Unfortunately, we have very little flexibility for a reason that I cannot discuss before Thursday. Should we still be able to meet on Thursday as planned then we will be able to brief you on that

item and you will understand the lack of flexibility. Sorry!

Philip Stupak
Director of Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

On Feb 28, 2023, at 5:19 PM, Pierre-Alexandre Houver <pahouver@garnault-associes.com> wrote:

Dear Philip,

I hope you are well.

We have a little issue. The CISA workshop is planned on Thursday morning and because of the lag, our agenda introduced a confusion in our planning.

Do we have any chance to meet tomorrow morning before 1pm? Or, can we move this from 11:00/12:00 to 12:00/13:00 ?

If not, we will contact CISA to work it out.

I apologize for this but be sure that our meeting is our priority.

Kind regards,

Pierre-Alexandre

Le 28 févr. 2023 à 10:08, Stupak, Philip
M. EOP/NCD

<(b) (6)> a écrit :

Dear Pierre-Alexandre,

Thank you for the note. I deleted MP Izard and reentered his information based on the shared passport. He should be good to enter. I have also submitted all the guests to clearance, and will alert you if any issues arise with entered information.

I can certainly cover the TikTok Ban. We would like to better understand the delegation's thoughts on the Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS) as I understand that EU Member State cyber experts and ENISA are likely meeting in the near future.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber Director
Executive Office of the President

(b) (6)

From: Pierre-Alexandre Houver
<pahouver@garnault-associes.com>
Sent: Tuesday, February 28, 2023 8:04 AM
To: Stupak, Philip M. EOP/NCD
<(b) (6)>
Cc: sgarnault@garnault-associes.com
Subject: Re: [EXTERNAL] Meeting proposition - French CyberTaskForce Delegation | February 27th to March 3rd

Dear Philip,

I hope this email finds you well.
I am contacting you regarding the meeting.
MP Alexis Izard has not put his middle name in the form. I tried to refill the form but it appears I cannot do it as it has already been submitted. I don't know if this can be problematic? (I'm attaching to this email his passeport).

Moreover, if possible of course, we would be more than interested to talk about the TikTok ban from government phones.

Thank you again!

I wish you a very nice day.

Kind regards,

Pierre-Alexandre Houver

<image001.jpg>

Le 28 févr. 2023 à 00:13, Pierre-Alexandre Houver
<pahouver@garnault-associes.com> a écrit :

Dear Philip,

Thank you very much!
I've just completed the form for every member of our delegation. Is it ok on your side?
Do not hesitate to tell me if you need additional information.
Please also find enclosed le list of the members of our delegation.

I remain at your entire disposal for any further information you may need.

Kind regards,

Pierre-Alexandre

<2023_CYBERTASKFORCE_DELEGATION.pdf>

Le 27 févr. 2023 à 14:36,
Stupak, Philip M. EOP/NCD

<(b) (6)>

> a écrit :

Dear Pierre-Alexandre,

Wonderful! We would like to welcome you to the White House complex and meet at the Eisenhower Executive Office Building. The visitor entrance is located at 17th Street NW and State Place NW (generally maps will find that location if you enter 1650 17th Street NW). I will meet you there at 9:45am and bring you to the room.

Each member of your delegation will need to complete this form: <https://events.whitehous>

[e.gov/AppointmentRsvpForm
?rid=PWMB7M6MR3](https://e.gov/AppointmentRsvpForm?rid=PWMB7M6MR3)

Everyone in the delegation needs to complete the form and names need to match what is printed on passports. Foreign visitors should enter "Washington" under the question about City of Residence and "District of Columbia" under the question about State of Residence. No need for a social security number, but please do enter passport numbers. Masks are only required if you are not vaccinated.

Given the tight turn around, please ask your delegation to complete the form as soon as possible, but no later than tomorrow at noon ET.

Please reach out with any questions.

Philip Stupak
Director Federal Cybersecurity
Office of the National Cyber
Director
Executive Office of the
President
(b) (6)

From: Pierre-Alexandre
Houver <pahouver@garnault-associates.com>
Sent: Monday, February 27,
2023 2:22 PM
To: Stupak, Philip M. EOP/NCD
<(b) (6)>
>
Cc: sgarnault@garnault-associates.com
Subject: Re: [EXTERNAL]
Meeting proposition - French

CyberTaskForce Delegation |
February 27th to March 3rd

Dear Philip,

Thank you very much for your answer! We would be very honored and happy to meet with Deputy National Cyber Director Neal Higgins.

Thursday, March 2nd from 10 am to 11 am would work perfectly for our delegation.

I suppose that you may need personal data for access. Would you need IDs number or any information in order to plan accesses?

Also, would it be possible too to confirm the location in order to plan transports on our side?

Again, thank you very much.

I wish you a very nice day.

Kind regards,

--

Pierre-Alexandre Houver
Advisor to the president

27 boulevard de Solférino,
35000 Rennes
+ 33 6 86 51 56
96 - [pahouver@garnault-
associes.com](mailto:pahouver@garnault-associes.com)

Le 27 févr. 2023 à 13:59,
Stupak, Philip M. EOP/NCD

<(b) (6)>
> a écrit :

Hello Sébastian,

Apologies for the delay—
your email came as we
departed for the Munich
Security Conference and
we have been sorting
schedules on our return.
Unfortunately, (Acting)
National Cyber Director
Kemba Walden is
unavailable to meet with
the delegation. Our
Deputy National Cyber
Director Neal Higgins is
available on Thursday,
March 2, between 10am-
12pm if that window
works for you. Does your
schedule permit an hour-
long meeting during that
window on Thursday?

Philip Stupak
Director Federal
Cybersecurity
Office of the National
Cyber Director
Executive Office of the
President
202-881-6385

Begin forwarded message:

From: Sébastien
Garnault
<sgarnault@garnault-associates.com>

Date: February 14,
2023 at 4:01:51 AM
EST

To: "Walden, Kemba
E. EOP/NCD"

(b) (6)

Cc: Pierre-Alexandre
Houver
<pahouver@garnault-associates.com>

**Subject: [EXTERNAL] Meeting
proposition - French
CyberTaskForce
Delegation |
February 27th to
March 3rd**

Dear Kemba,

I hope this mail will find
you well.

I am writing this email
following a discussion
with **Mr Vincent Voci**,
Vice-President at the US
Chamber of Commerce. As
president of the French
CyberTaskForce, we are
currently planning to come
as a parliamentary
delegation to Washington
D.C. from February 27th to
March 3rd. Composed of
French Members of
Parliaments, Civil servants
and private sector decision-
makers, we are coming to
the US to meet our
colleagues and
counterparts involved in
technologies, cyber and
space.

In this context, we would
be particularly honored to
meet you for an exchange
of views focused on
Cyberdefense. **We
would be very
honored to meeting
you during our stay
in D.C.**

As you know, cyber-
attacks target large, small
and critical organizations.
However, addressing these
threats become more and
more complex for them as
skills, materials and
awareness are lacking.
Therefore, we would be
more than interested to
have a 1 hour meeting with
you to have a discussion on
how US and France tackle
these challenges and are

working on developing our common resilience into cyberspace. For your complete information, we will also meet CISA on these issues.

Members of the delegation:

1. **Ms Constance Le Grip**, Member of Parliament, Second Vice-President of the Parliamentary Intelligence Delegation - Co-head of delegation
2. **Mr Sébastien Garnault**, Founder of the French Cyber Task Force, founder of Paris Cyber Summit - Co-head of Delegation
3. **Mr Alexis Izard**, Member of Parliament, author of the information report "Investing for France 2030" for the Finance programming Law for 2023
4. **Mr Robin Reda**, Member of Parliament, member of the committee for Finance
5. **Ms Constance Nebbula**, Vice-President « Digital and Cyber » of Pays de la

- Loire Regiona
l Council
6. **Mr Florent
Kirchner**, He
ad of the
French
national
cybersecurity
strategy -
Prime
minister
 7. **Mr Bruno
Charrat**, Dep
uty Director
of
Technological
Research at the
CEA -
Atomic
Energy
Commission,
representative
of the
Alliance for
Digital Trust
(French
cybersecurity
professional
association)
 8. **Mr Pierre-
Alexandre
Houwer**, Adv
isor at
Garnault &
Associés
 9. **Mr Baptiste
Robert**, CEO
at Predicta
Lab

I warmly thank you and I
stay personally at your
entire disposal, and for
your team, for any
additional information you
may need.

With best wishes,
Sébastien Garnault

--

Sébastien Garnault
Founder of
CyberTaskForce
and Paris Cyber
Summit

President of
Garnault &
Associés

27, boulevard
Solférino - F-35 000
Rennes
+33 6 80 71 60 56
- sgarnault@garnault-associes.com
[@SebGarnault](#) - [Profil LinkedIn](#)