

Sarbanes Oxley Compliance Professionals Association (SOXCPA)  
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA  
Tel: 202-449-9750 Web: [www.sarbanes-oxley-association.com](http://www.sarbanes-oxley-association.com)



## *Sarbanes Oxley News, January 2022*

Dear members and friends,

We will start with Jerome H. Powell's nomination hearing before the Committee on Banking, Housing, and Urban Affairs. He said that the Fed could raise interest rates to manage inflation, as the rising costs of housing, gas, food and furniture are pinching shoppers and tanking consumer confidence.



### **Nomination hearing**

Chairman Brown, Ranking Member Toomey, and other members of the Committee, thank you for the opportunity to appear before you today.

I would like to thank President Biden for nominating me to serve a second term as Chair of the Board of Governors of the Federal Reserve System.

I would also like to thank my colleagues throughout the Federal Reserve System for their dedication, perseverance, and tireless work on behalf of the American people.

Their commitment and expertise were essential to the Fed's response to the COVID-19 crisis and remain vital to the implementation of monetary policy

as our economy continues to progress. Particular thanks go to my wife, Elissa Leonard, and our three children, Susie, Lucy, and Sam. Their love and support make possible everything I do. My five siblings are all watching, and we are thinking of each other and of our parents today with love and gratitude.

Four years ago, when I sat before this Committee, few could have predicted the great challenges that would soon become ours to meet.

On the eve of the pandemic, the U.S. economy was enjoying its 11th year of expansion, the longest on record. Unemployment was at 50-year lows, and the economic benefits were reaching those most on the margins.

No obvious financial or economic imbalances threatened the ongoing expansion. But this attractive picture turned virtually overnight as the virus swept across the globe.

The initial contraction was the fastest and deepest on record, but the pain could have been much worse. As the pandemic arrived, our immediate challenge was to stave off a full-scale depression, which would require swift and strong policy actions from across government.

Congress provided by far the fastest and largest response to any postwar economic downturn. At the Federal Reserve, we used the full range of policy tools at our disposal. We moved quickly to restore vital flows of credit to households, communities, and businesses and to stabilize the financial system.

These collective policy actions, the development and availability of vaccines, and American resilience worked in concert, first to cushion the pandemic's economic blows and then to spark a historically strong recovery.

Today the economy is expanding at its fastest pace in many years, and the labor market is strong.

As always, challenges remain. Both the initial shutdown and the subsequent reopening of the economy were without precedent.

The economy has rapidly gained strength despite the ongoing pandemic, giving rise to persistent supply and demand imbalances and bottlenecks, and thus to elevated inflation.

We know that high inflation exacts a toll, particularly for those less able to meet the higher costs of essentials like food, housing, and transportation.

We are strongly committed to achieving our statutory goals of maximum employment and price stability.

We will use our tools to support the economy and a strong labor market and to prevent higher inflation from becoming entrenched.

We can begin to see that the post-pandemic economy is likely to be different in some respects. The pursuit of our goals will need to take these differences into account. To that end, monetary policy must take a broad and forward-looking view, keeping pace with an ever-evolving economy.

Over the past four years, my colleagues and I have continued the work of our predecessors to ensure a strong and resilient financial system.

We increased capital and liquidity requirements for the largest banks—and currently, capital and liquidity levels at our largest, most systemically important banks are at multidecade highs.

We worked to improve the public's access to instant payments, intensified our focus and supervisory efforts on evolving threats such as climate change and cyberattacks, and expanded our analysis and monitoring of financial stability. We will remain vigilant about new and emerging threats.

We also updated our monetary policy framework, drawing on insights from people and communities across the country, to reflect the challenges of conducting policy in an era of persistently low interest rates.

Congress has assigned the Federal Reserve important goals and has given us considerable independence in using our tools to achieve them. In our democratic system, that independence comes with the responsibility of transparency and clear communication, to keep the public informed and enable effective legislative oversight.

That duty takes on even greater significance when the Fed must take extraordinary actions in times of crisis. In order to facilitate that transparency, and to earn your trust and that of the American people, I have made it a priority to meet regularly and frequently with you and your elected colleagues. I commit to continuing that practice if I am confirmed to another term.

The Federal Reserve works for all Americans. We know our decisions matter to every person, family, business, and community across the country. I am committed to making those decisions with objectivity, integrity, and impartiality, based on the best available evidence, and in the long-standing tradition of monetary policy independence.

That pledge lies at the heart of the Fed's mission and is one we all make when we answer the call to public service. I make it here again, with force and without reservation.

Everything we do at the Federal Reserve is in pursuit of the goals set for us by Congress. I am honored to have worked in service to those ends since I joined the Fed in 2012, and as Chair for the past four years.

Thank you. I look forward to your questions.

## Staff Guidance

Form AP, Auditor Reporting of Certain Audit Participants, and Related Voluntary Audit Report Disclosure Under AS 3101, The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion - Updated as of Dec. 17, 2021



### A. Filing Requirements

#### 1. General Requirements

*General.* Each registered public accounting firm must provide information about engagement partners and accounting firms that participate in audits of issuers by filing a Form AP, Auditor Reporting of Certain Audit Participants ("Form AP"), for each audit report issued by the firm for an issuer.

Form AP is due by the 35th day after the date the audit report is first included in a document filed with the Securities and Exchange Commission ("SEC" or "Commission"), subject to the shorter filing deadline that applies when the audit report is first included in a Securities Act registration statement (described below).

*Example:* A registered firm issues its audit report on the financial statements of Company A on February 28. Company A files its annual report on Form 10-K (the first SEC filing to include the audit report) on March 1. Form AP is due not later than April 5 (35 days after March 1).

*Securities Act Registration Statements.* If the audit report is first included in a registration statement filed with the SEC under the Securities Act, the firm is required to file Form AP by the 10th day after the date the audit report is first included in a document filed with the SEC.

*Example—IPO:* On March 20, Company B, an emerging growth company ("EGC"), confidentially submits a draft Securities Act registration statement for SEC staff review.

The firm is not required to file Form AP in connection with such a submission. On July 18, Company B files a Securities Act registration statement that is the first SEC filing to include the audit report on the financial statements.

The firm is required to file Form AP by July 28.

*Example—Mutual Fund Formation:* On June 6, a Securities Act registration statement is filed in connection with the formation of Fund C, an open-end mutual fund. The registration statement is the first SEC filing

to include the audit report on the financial statements of Fund C. The firm is required to file Form AP by June 16.

*Application of Filing Deadline in Other Circumstances.*

*Example—Contemporaneous Filing of Annual Report and Registration Statement:* On March 1, Company D files both its annual report on Form 10-K, containing ABC Audit Firm's audit report, and a registration statement on Form S-3, incorporating the Form 10-K by reference.

Because of the incorporation by reference, the Form 10-K would be considered to be filed prior to the registration statement for purposes of Rule 3211 deadlines, and the filing deadline applicable to Form AP would be 35 days after the filing of Form 10-K, not 10 days after the filing of Form S-3.

*Example—Reverse Merger:* Company E, a shell company, acquires Operating Company X, a private company, on October 14 and files a current report on Form 8-K, including the audited financial statements of Operating Company X, on October 18.

There is no requirement for the auditor of Operating Company X to file Form AP in connection with the filing of Form 8-K because Operating Company X is not an issuer.

Form AP would be due in connection with the next filing of an audit report for Company E, for example, with the filing of Company E's annual report on Form 10-K.

The report: [https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/standards/documents/2021-12-17-form-ap-staff-guidance.pdf?sfvrsn=52d4323d\\_4](https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/standards/documents/2021-12-17-form-ap-staff-guidance.pdf?sfvrsn=52d4323d_4)

## Erica Y. Williams Sworn in as PCAOB Chair



The Public Company Accounting Oversight Board (PCAOB) announced that Erica Y. Williams was sworn in as Chair. The U.S. Securities and Exchange Commission (SEC) conducted the swearing-in ceremony virtually.



“In our dynamic and evolving capital markets, the PCAOB’s mission to protect investors and further the public interest is extremely important,” said Chair Williams.

“I am honored to take up this mission and to lead this organization’s dedicated, talented staff. Together, we have an extraordinary opportunity to build trust through robust oversight and engagement.”

Appointed by the SEC on November 8, 2021, Chair Williams’ initial term will run through **October 24, 2024**.

Chair Williams joins the PCAOB from Kirkland & Ellis LLP, where she was a litigation partner. Previously, she was a Special Assistant and Associate Counsel to President Barack Obama, advising the president and his senior advisors on legal and constitutional issues involving economic policy, financial regulation and reform, financial technology, trade, intellectual property, and data protection and privacy.

Before that, Chair Williams spent 11 years at the SEC serving as Deputy Chief of Staff for three chairs. In this role, she oversaw all aspects of the SEC’s operations and served as a senior legal advisor to the SEC chair on regulatory policy and rulemakings, enforcement, compliance examinations, agency management and strategy.

Earlier in her career, Chair Williams served as Assistant Chief Litigation Counsel in the SEC’s Division of Enforcement Trial Unit, where she investigated and litigated numerous complex, high-profile matters. Chair Williams earned both a J.D. and a B.A. from the University of Virginia.

“On behalf of all of my PCAOB colleagues, I offer sincere thanks to Board Member DesParte for his steady leadership as Acting Chairperson,” added Chair Williams. “I look forward to working with Duane and my other fellow Board members as we continue the critical work of the PCAOB.”

## SEC Awards Over \$13 Million To Whistleblower



The Securities and Exchange Commission announced an award of more than \$13 million to a whistleblower whose information and assistance prompted the opening of an investigation and significantly contributed to the success of an SEC enforcement action.

The whistleblower promptly alerted SEC staff to an ongoing fraud and provided extensive assistance to SEC staff by meeting in person and helping the staff understand the mechanics of the fraudulent scheme. The whistleblower's information also helped the Commission obtain emergency relief to minimize investor losses.

"Today's whistleblower provided significant information that alerted SEC staff to ongoing fraud, which had caused and was likely to continue to cause substantial injury to the financial interests of investors," said Creola Kelly, Chief of the SEC's Office of the Whistleblower. "Whistleblowers who provide information swiftly can not only save SEC staff's time and resources, but also help minimize potential investor losses."

The SEC has awarded approximately \$1.2 billion to 238 individuals since issuing its first award in 2012. All payments are made out of an investor protection fund established by Congress that is financed entirely through monetary sanctions paid to the SEC by securities law violators.

No money has been taken or withheld from harmed investors to pay whistleblower awards. Whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action.

Whistleblower awards can range from 10 percent to 30 percent of the money collected when the monetary sanctions exceed \$1 million.

As set forth in the Dodd-Frank Act, the SEC protects the confidentiality of whistleblowers and does not disclose any information that could reveal a whistleblower's identity.

For more information about the whistleblower program and how to report a tip, visit [www.sec.gov/whistleblower](http://www.sec.gov/whistleblower)

## *Office of the Whistleblower*

Assistance and information from a whistleblower who knows of possible securities law violations can be among the most powerful weapons in the law enforcement arsenal of the Securities and Exchange Commission.

Through their knowledge of the circumstances and individuals involved, whistleblowers can help the Commission identify possible fraud and other violations much earlier than might otherwise have been possible.

That allows the Commission to minimize the harm to investors, better preserve the integrity of the United States' capital markets, and more swiftly hold accountable those responsible for unlawful conduct.

The Commission is authorized by Congress to provide monetary awards to eligible individuals who come forward with high-quality original information that leads to a Commission enforcement action in which over \$1,000,000 in sanctions is ordered. The range for awards is between 10% and 30% of the money collected.

The Office of the Whistleblower was established to administer the SEC's whistleblower program. We understand that the decision to come forward with information about securities fraud or other wrongdoing is not one taken lightly, and we are here to answer any questions you may have. You can reach the Office of the Whistleblower at (202) 551-4790.

# The Double-Edged Sword of AI: Enabler of Disinformation



<b>Introduction</b> .....	<b>6</b>
<b>Content preparation</b> .....	<b>9</b>
Automated web data scraping .....	9
Automatic generation of text .....	10
Deepfakes: images, audio, video .....	12
<b>Spreading disinformation</b> .....	<b>17</b>
Bots, sock puppets, cyborgs .....	17
Disinformation enabled by social networks and data brokers .....	19
<b>Possible future trends for AI-powered disinformation</b> .....	<b>21</b>
<b>Conclusions</b> .....	<b>24</b>
<b>Literature</b> .....	<b>27</b>

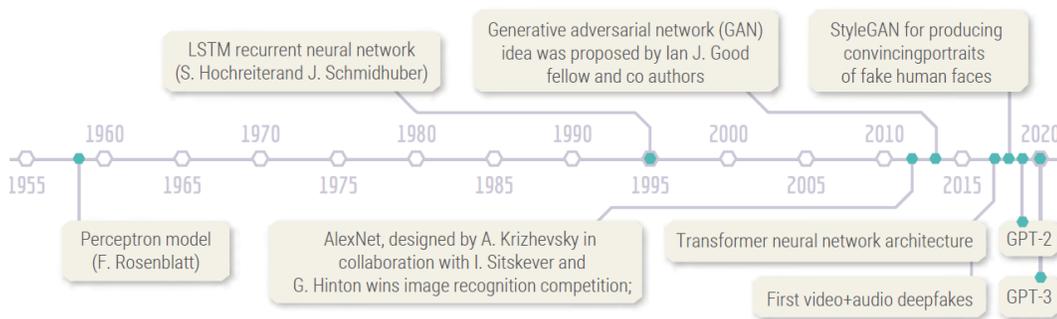
## *Abstract*

The tendency to consume news on social media platforms has greatly increased over the last decade. Information can now be disseminated quickly, cheaply, and with easy access for consumers; this has rapidly boosted decentralized news production, often without editorial oversight.

Adversarial agents are exploiting this situation to spread disinformation. Over the past ten years, the field of Artificial Intelligence (AI)/Machine Learning (ML) has experienced unprecedented growth in the development of applications for the automation of text, and the recognition and generation of visual and audio data.

Do these burgeoning AI capabilities boost the abilities of malicious actors to manipulate crowds? AI now plays a vital role in generating synthetic content and enables the efficient micro-targeting used on social media platforms to spread disinformation messages, including hyper-realistic synthetic images, videos, audios, and text.

This rather technical article has been written to inform practitioners, policymakers, and AI enthusiasts in NATO about how AI/ML technologies can be used to shape disinformation.



**Figure 1.** Some AI milestones relevant to the automated generation of disinformation content.

To read more: <https://stratcomcoe.org/publications/the-double-edged-sword-of-ai-enabler-of-disinformation/221>

## Why vulnerabilities are like buses

How organisations can address the growing trend in which multiple vulnerabilities within a single product are exploited over a short period.



There's an old saying that you wait ages for a bus, and then several come at once.

A growing trend is the mass exploitation of a critical vulnerability in a product, followed shortly after by further critical vulnerabilities (and often 'in-the-wild' exploitation) in the same product. Organisations will have worked hard to push out-of-band patches for the initial vulnerability, only to have to repeat the process later when new vulnerabilities appear.

In this blog, we'll explore the factors driving this, and explain how organisations can better protect the software they've just patched from exploitation of future vulnerabilities.

### *Why does it happen?*

A hostile actor looking for a usable vulnerability (or a security researcher identifying material for a publication or conference) only needs to find a single vulnerability in a product.

Once identified, the incentive to keep looking for others in the same product falls away. Products and services are very complex, and vendors or bug-bounty researchers are unlikely to find all the security flaws they contain.

When responding to a mass exploitation (or when vendors only have a fixed amount of time to address a flaw before an imposed deadline), they must focus on patching the immediate issue, rather than in-depth remediation of more fundamental flaws.

Fixing these underlying problems – hopefully – starts in parallel, but it can take months of work to retire or rewrite dangerous flaws in a product.

When a high-impact vulnerability is mass exploited and makes the news, it suggests the software contains other exploitable flaws. Security researchers or threat actors may then decide that it's worth further research.

They might familiarize themselves with the technology and go on to find new security issues, which they then release to the vendor – or if their intentions are malign, use as an exploit. This can lead to another wave of exploitation. In some cases, an organisation may not be affected in the first

wave, but is later compromised when the second (or third) vulnerability appears.

Even if the vendor has made initial efforts to improve a product's security, it may still take longer to find and fix more fundamental issues than it takes threat actors – who have now smelt blood – to find and exploit them.

*What can organisations do?*

The rush to apply patches is unfortunately necessary once 'in-the-wild' exploitation is observed. The NCSC's advice remains for organisations to install security updates as soon as it's practicable.

However, in the immediate aftermath, defenders might consider how they can better protect the software they've just patched from future exploitation, when a patch isn't available or isn't yet applied.

An effective way to protect software is to reduce the attack surface by turning off or limiting software functionality.

This can include:

- turning off interfaces or protocols not in use
- where possible ensuring admin interfaces are not exposed to the internet
- disabling legacy components or settings
- upgrading or replacing legacy software where patches are no longer available
- restricting network traffic to and from the device
- reviewing authentication and authorisation for the device
- making sure future patching happens as soon as is practicable
- crucially, ensuring that the system isn't unpatchable in the first place.

Organisations can also use the case studies emerging from real-world vulnerability exploitations to consider whether their own monitoring system would have detected activity on software and devices, and make adjustments where necessary.

---

*Never let a good crisis go to waste*

If considered strategically, the need to apply out-of-band patches in a high-pressure situation can give an organisation the required momentum to harden its internet-exposed software. This can help shift an organisation's security mindset from mostly reactive to more proactive, ultimately improving its fundamental network security.

A high-profile exploitation (such as the 'Proxyshell' issues in Microsoft Exchange Server mentioned earlier, or the current critical vulnerability affecting the Apache Log 4j 2 library) often brings considerable interest from an organisation's senior decision-makers.

This can then provide the impetus to secure the senior sponsorship and financial buy-in for slower, but equally important longer-term security projects, which might be harder to 'sell' in normal circumstances.

To read more: <https://www.ncsc.gov.uk/blog-post/why-vulnerabilities-are-like-buses>

## Mitigating Log4Shell and Other Log4j-Related Vulnerabilities



CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom have released a joint Cybersecurity Advisory in response to multiple vulnerabilities in Apache's Log4j software library. You may visit: <https://www.cisa.gov/uscert/ncas/alerts/aa21-356a>

### Technical Details

#### Log4Shell

**Log4Shell**, disclosed on December 10, 2021, is a remote code execution (RCE) vulnerability affecting Apache's Log4j library, versions 2.0-beta9 to 2.14.1. The vulnerability exists in the action the Java Naming and Directory Interface (JNDI) takes to resolve variables. Affected versions of Log4j contain JNDI features—such as message lookup substitution—that do not protect against adversary-controlled Lightweight Directory Access Protocol (LDAP), Domain Name System (DNS), and other JNDI-related endpoints.

An adversary can exploit Log4Shell by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows the adversary to take full control over the system. The adversary can then steal information, launch ransomware, or conduct other malicious activity.

#### CVE-2021-45046

**CVE-2021-45046**, disclosed on December 13, 2021, enables a remote attacker to cause RCE, a denial-of-service (DoS) condition, or other effects in certain non-default configurations. This vulnerability affects all versions of Log4j from 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0. In response, Apache released Log4j version 2.16.0 (Java 8).

#### CVE-2021-45105

**CVE-2021-45105**, disclosed on December 16, 2021, enables a remote attacker to cause a DoS condition or other effects in certain non-default configurations. According to Apache, when the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, `$$${ctx:loginId}`), attackers with control over Thread Context Map (MDC) input data can craft malicious input data that contains a recursive lookup, resulting in a `StackOverflowError` that will terminate the process. In response, Apache released Log4j version 2.17.0 (Java 8).

#### Impact

Log4Shell and CVE-2021-45046—rated as critical vulnerabilities by Apache—are severe because Java is used extensively across IT and OT platforms, they are easy to exploit, and applying mitigations is resource intensive. Log4Shell is especially critical because it allows malicious actors to remotely run code on vulnerable networks and take full control of systems.

According to public reporting, exploitation of Log4Shell began on or around December 1, 2021, and a proof-of-concept exploit is publicly available for this vulnerability. The FBI has observed attempted exploitation and widespread scanning of the Log4j vulnerability to gain access to networks to deploy cryptomining and botnet malware. The FBI assesses this vulnerability may be exploited by sophisticated cyber threat actors and incorporated into existing cyber criminal schemes that are looking to adopt increasingly sophisticated obfuscation techniques. According to public reporting<sup>1</sup>, CVE-2021-45046 is being actively exploited as well.

CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK assess that exploitation of these vulnerabilities, especially Log4Shell, is likely to increase and continue over an extended period. Given the severity of the vulnerabilities and likely increased exploitation, CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK strongly urge all organizations to apply the recommendations in the Mitigations section to identify, mitigate, and update affected assets.

For more information on these vulnerabilities, see the [Apache Log4j Security Vulnerabilities](#) webpage.

Malicious cyber actors are actively scanning networks to potentially exploit CVE-2021-44228 (known as “Log4Shell”), CVE-2021-45046, and CVE-2021-45105 in vulnerable systems. According to public reporting, Log4Shell and CVE-2021-45046 are being actively exploited.

This advisory expands on CISA's previously published guidance, drafted in collaboration with industry members of CISA's Joint Cyber Defense Collaborative (JCDC), by detailing recommended steps that vendors and organizations with information technology, operational technology /industrial control systems, and cloud assets should take to respond to these vulnerabilities.

CISA, FBI, NSA, the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber

Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) assess that exploitation of these vulnerabilities, especially Log4Shell, is likely to increase and continue over an extended period. CISA and its partners strongly urge all organizations to review AA21-356A: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities for detailed mitigations.

You may visit: <https://www.cisa.gov/uscert/ncas/current-activity/2021/12/22/mitigating-log4shell-and-other-log4j-related-vulnerabilities>

## From battling COVID-19 and cancer to searching for signs of ancient life on Mars, see Los Alamos' top stories from 2021



Despite the year's many challenges (and, in some cases, because of them), there were some incredible scientific and technological innovations out of Los Alamos in 2021. Here's a look back at just a few of them.

### Mission to Mars!

#### *Perseverance rover takes New Mexico to Mars*

When NASA's Mars Perseverance rover touched down on the surface of Mars on Feb. 18, a bit of New Mexico landed along with it, thanks to work done at Los Alamos National Laboratory. Watch this video to learn about the rover's first two days on Mars.

#### *New research shows that Mars did not dry up all at once*

While attention has been focused on the Perseverance rover that landed on Mars last month, its predecessor Curiosity continues to explore the base of Mount Sharp on the Red Planet and is still making discoveries. Research published in the journal "Geology" shows that Mars had drier and wetter eras before drying up completely about 3 billion years ago.

#### *First results from Perseverance mission show evidence of flash floods on Mars*

New images from the Perseverance mission show evidence of delta and flood deposits in Jezero Crater on Mars, indicating that there were massive flash floods as well as periods of stability on the Red Planet. The deltas are an ideal place to search for signs of ancient life.

#### *What does music sound like on Mars*

The atmosphere is different on Mars, which means that sound travels differently. Watch this video to hear what music sounds like on Mars versus Earth!

### Battling COVID-19

*Vaccine development software shows promise in influenza effort, could help defeat coronavirus*

A novel computer algorithm that could create a broadly reactive influenza vaccine for swine flu also offers a path toward a pan-influenza vaccine and possibly a pan-coronavirus vaccine as well, according to a new paper published in "Nature Communications."

*Simulations reveal how dominant SARS-CoV-2 strain binds to host, succumbs to antibodies*

Large-scale supercomputer simulations at the atomic level show that the dominant G form variant of the COVID-19-causing virus is more infectious partly because of its greater ability to readily bind to its target host receptor in the body, compared to other variants.

These research results from a Los Alamos National Laboratory–led team illuminate the mechanism of both infection by the G form and antibody resistance against it, which could help in future vaccine development. Watch this video to learn more.

*Forecasting the spread of COVID*

Los Alamos scientists used computer modeling to forecast the spread of COVID-19 through communities and help decision-makers determine which mitigation strategies were the most effective.

## [Moving toward a clean-energy future](#)

*Advancing fuel cell technology*

The U.S. transportation industry is the nation's largest generator of greenhouse gases, accounting for nearly one-third of climate-warming emissions. To move towards a clean-energy future, developing zero-emissions technologies for heavy-duty vehicles is critical.

A new partnership comprising Los Alamos National Laboratory, Advent Technology Holdings Inc., Brookhaven National Laboratory, and the National Renewable Energy Laboratory (NREL) will work over the next few years to bring to market high-temperature proton exchange membrane (HT-PEM) fuel cells that convert hydrogen and other renewable fuels into electricity.

*New fabrication method paves way to large-scale production of perovskite solar cells*

A new, simpler solution for fabricating stable perovskite solar cells overcomes the key bottleneck to large-scale production and commercialization of this promising renewable-energy technology, which has remained tantalizingly out of reach for more than a decade.

## Using climate science to assess our changing world

### *Freshwater outflow from Beaufort Sea could alter global climate patterns*

The Beaufort Sea, the Arctic Ocean's largest freshwater reservoir, has increased its freshwater content by 40% over the last two decades, putting global climate patterns at risk. A rapid release of this freshwater into the Atlantic Ocean could wreak havoc on the delicate climate balance that dictates global climate.

### *Colorado River basin due for more frequent, intense hydroclimate events*

In the vast Colorado River basin, climate change is driving extreme, interconnected events among earth-system elements such as weather and water. These events are becoming both more frequent and more intense and are best studied together, rather than in isolation, according to new research.

### *Antarctica remains the wild card for sea-level rise estimates through 2100*

A massive collaborative research project covered in the journal "Nature" offers projections to the year 2100 of future sea-level rise from all sources of land ice, offering the most complete projections created to date.

### *Why arctic soil can go slip-sliding away*

Slow-moving arctic soils form patterns that, from a distance, resemble those found in common fluids such as drips in paint and birthday cake icing. Los Alamos researchers and their collaborators analyzed existing arctic soil formations and compared them to viscous fluids, determining that there is a physical explanation for this pattern that is common to both Earth and Mars landscapes.

### *Studying climate change in the Arctic*

In the Arctic, climate shifts are rapidly changing ecosystems, resulting in large feedbacks between snow, vegetation, and permafrost. Thicker snow leads to warmer permafrost because a deeper snowpack will insulate the ground from the frigid Arctic winter. Because shrubs tend to capture and hold snow, researchers find the warmest temperatures beneath the shrubs, along with warming permafrost. In fact, underneath the shrubs and deep snow, windows — called taliks — into the permafrost will develop, allowing more water, energy, and nutrients to flow into the permafrost, speeding up the rate of warming and thawing.

## *Global warming, not just drought, drives bark beetles to kill more ponderosa pines*

In California's Sierra Nevada, western pine beetle infestations amped up by global warming were found to kill 30% more ponderosa pine trees than the beetles do under drought alone. A new supercomputer modeling study hints at the grim prospect of future catastrophic tree die-offs and offers insights for mitigating the combined risk of wildfires and insect outbreaks.

### *How does climate change affect disease spread?*

Climate change can make it easier for diseases to jump from animals to humans. Los Alamos National Laboratory researchers Andrew Bartlow, Jeanne Fair and Carrie Manore discuss the impact climate change has on infectious disease spread.

## [Understanding more about wildfires](#)

### *Prescribed burns and other low-intensity fires are highly responsive to changes in winds*

Scientists at Los Alamos National Laboratory and partners have used modeling to highlight the large impact that small changes in wind conditions can have on low-intensity fires or prescribed burns. Conducting safe prescribed fires depends on anticipating the range of potential fire behavior associated with complex wind conditions.

### *Probing wet fire smoke in clouds: Can water intensify the Earth's warming?*

A first-of-its-kind instrument that samples smoke from megafires and scans humidity will help researchers better understand the scale and long-term impact of fires — specifically how far and high the smoke will travel; when and where it will rain; and whether the wet smoke will warm the climate by absorbing sunlight.

### *Understanding pyrocumulonimbi, aka 'fire clouds'*

In recent years, megafires and their blanketing haze have become an increasingly familiar sight, along with the towering thunderheads of smoke that form above them. Yet we're only beginning to learn what causes those awe-inspiring "fire clouds," what's in them and what effects they have on weather on climate. Through a combination of field observations, experimental work in the laboratory and computer modeling at local to global scales, our team at Los Alamos National Laboratory is making progress in understanding the mechanisms and climate impacts of

pyrocumulonimbus from recent megafires in British Columbia (2017) and Australia (2019-2020).

## Making strides in machine learning, AI

### *Machine learning blazes path to reliable near-term quantum computers*

Using machine learning to develop algorithms that compensate for the crippling noise endemic on today's quantum computers offers a way to maximize their power for reliably performing actual tasks, according to a new paper.

### *Machine learning aids in simulating dynamics of interacting atoms*

A revolutionary machine-learning (ML) approach to simulate the motions of atoms in materials such as aluminum is described in "Nature Communications" journal. This automated approach to "interatomic potential development" could transform the field of computational materials discovery.

### *New AI tool makes vast data streams intelligible and explainable*

Making sense of vast streams of big data is getting easier, thanks to an artificial-intelligence tool developed at Los Alamos National Laboratory. SmartTensors sifts through millions of millions of bytes of diverse data to find the hidden features that matter, with significant implications from health care to national security, climate modeling to text mining, and many other fields.

### *New AI tool tracks evolution of COVID-19 conspiracy theories on social media*

A new machine-learning program accurately identifies COVID-19-related conspiracy theories on social media and models how they evolved over time — a tool that could someday help public health officials combat misinformation online.

### *Machine learning model generates realistic seismic waveforms*

A new machine-learning model that generates realistic seismic waveforms will reduce manual labor and improve earthquake detection, according to a study published recently in JGR Solid Earth.

### *Machine learning refines earthquake detection capabilities*

Researchers at Los Alamos National Laboratory are applying machine learning algorithms to help interpret massive amounts of ground

deformation data collected with Interferometric Synthetic Aperture Radar (InSAR) satellites; the new algorithms will improve earthquake detection.

### *Science, AI help unlock green energy in northwest New Mexico*

A group of Navajo entrepreneurs in Tohatchi have had their eye on the business potential of an oil-exploration well drilled in the 1950s, but they're not considering fossil fuel production. The well produces water heated by hidden deep geologic processes. As a geothermal energy source, the well might help power the group's plans to create a long-term food-water-energy nexus on the Navajo Nation, stimulating the local economy while helping New Mexico transition to a carbon-free energy portfolio.

### [Exploring the next frontier of computing: Quantum](#)

#### *Lack of symmetry in qubits can't fix errors in quantum computing, but might explain matter/antimatter imbalance*

A team of quantum theorists seeking to cure a basic problem with quantum annealing computers — they have to run at a relatively slow pace to operate properly — found something intriguing instead.

While probing how quantum annealers perform when operated faster than desired, the team unexpectedly discovered a new effect that may account for the imbalanced distribution of matter and antimatter in the universe and a novel approach to separating isotopes.

#### *Software evaluates qubits, characterizes noise in quantum annealers*

High-performance computer users in the market for a quantum annealing machine or looking for ways to get the most out of one they already have will benefit from a new, open-source software tool for evaluating these emerging platforms at the individual qubit level.

#### *New quantum research gives insights into how quantum light can be mastered*

A team of scientists at Los Alamos National Laboratory propose that modulated quantum metasurfaces can control all properties of photonic qubits, a breakthrough that could impact the fields of quantum information, communications, sensing and imaging, as well as energy and momentum harvesting. The results of their study were released yesterday in the journal "Physical Review Letters," published by the American Physical Society.

#### *Quantum machine learning hits a limit*

A new theorem from the field of quantum machine learning has poked a major hole in the accepted understanding about information scrambling. Watch this video to learn more.

## Narrowing down the neutrino

### *Physics experiment boosts evidence for sterile neutrinos*

Analysis of results from an experiment called MiniBooNE at Fermilab has provided yet more evidence that particles called “sterile neutrinos” could indeed exist, supporting results from a 1990s Los Alamos National Laboratory experiment that indicated an update to the Standard Model of physics might be in order.

### *Neutron measured with greatest-ever precision*

The neutron, one of the three primary particles comprising everyday matter, was discovered in 1932. But despite all the advances in physics in the last 89 years, the exact life expectancy of the neutron has managed to remain elusive, even disputed.

An experiment at Los Alamos National Laboratory with twice the precision of previous efforts has now measured the neutron lifetime at 877.75 seconds, with record uncertainty of less than one-tenth of one percent.

## Developed radioisotopes to fight cancer and diseases

### *Los Alamos generator system delivers large radiation doses directly to cancer cells*

Improved options for cancer treatment are on the way, thanks to a new system developed at Los Alamos National Laboratory for producing alpha-emitting medical radioisotopes intended to target and overpower diseased tissue while sparing the healthy tissue around it.

### *Combating drug resistant infections with radioisotopes*

Researchers at Los Alamos National Laboratory have developed a promising new approach for diagnosing and treating drug-resistant pathogenic microorganisms that uses bacteria-specific siderophores to convey a treatment molecule directly to a pathogen. Siderophores are “iron carriers,” which are molecules produced by microorganisms such as fungi and bacteria that transport iron across cell membranes.

## [Answered questions about our galaxy](#)

### *HAWC Gamma Ray Observatory discovers origin of highest-energy cosmic rays in the galaxy*

A long-time question in astrophysics appears to finally be answered, thanks to a collection of large, high-tech water tanks on a mountainside in Mexico. The High-Altitude Water Cherenkov (HAWC) data shows that the highest-energy cosmic rays come not from supernovae, but from star clusters.

### *Boundary of heliosphere mapped for the first time*

For the first time, the boundary of the heliosphere has been mapped, giving scientists a better understanding of how solar and interstellar winds interact. Watch this video to learn more.

### *3D simulations improve understanding of energetic-particle radiation and help protect space assets*

A team of researchers used 3D particle simulations to model the acceleration of ions and electrons in a physical process called magnetic reconnection. The results could contribute to the understanding and forecasting of energetic particles released during magnetic reconnection, which could help protect space assets and advance space exploration.

## [Other top stories](#)

### *B61-12 bomb reaches major milestone*

A major milestone has been achieved with the recent delivery of the first production unit (FPU) of the B61-12, meaning the refurbished bomb is on track for full-scale production in May 2022. The bomb has been undergoing a life extension program for more than nine years. Los Alamos and Sandia National Laboratories are the design agencies for the project, with Los Alamos also being responsible for producing detonators and other classified components.

### *Integrating diverse satellite images to sharpen our picture of activity on Earth*

At Los Alamos National Laboratory, we've developed a flexible mathematical approach to identify changes in satellite image pairs collected from different satellite modalities, or sensor types that use different sensing technologies, allowing for faster, more complete analysis.

It's easy to assume that all satellite images are the same and, thus, comparing them is simple. But the reality is quite different. Hundreds of different imaging sensors are orbiting the Earth right now, and nearly all take pictures of the ground in a different way from the others. Watch this video to learn more.

*Using supercomputers to reveal how X chromosomes fold, deactivate*

Using supercomputer-driven dynamic modeling based on experimental data, researchers can now probe the process that turns off one X chromosome in female mammal embryos.

This new capability is helping biologists understand the role of RNA and the chromosome's structure in the X inactivation process, leading to a deeper understanding of gene expression and opening new pathways to drug treatments for gene-based disorders and diseases. Watch this video to learn more.

*Newly identified tiny mineral named for Los Alamos and U. Wisconsin scientists*

A vanishingly tiny mineral is being named for two scientists who have revolutionized the analysis of mineral samples. Xuite (pronounced "zoo-ite"), the newest member of the nano-mineral pantheon, is named in honor of Los Alamos National Laboratory mineralogist Hongwu Xu and the University of Wisconsin's Huifang Xu.

*Optical biosensor device aids in biomarker identification*

Work at Los Alamos National Laboratory, in conjunction with its research partners, provides valuable new insights into the diagnosis of tuberculosis (TB) using blood tests.

A paper in the journal "PLOS ONE" demonstrates the role that host-pathogen interactions play in detecting key biomarkers in blood, facilitating the diagnosis of disseminated or sub-clinical TB disease.

*Discovery of new material could someday aid in nuclear nonproliferation*

A newly discovered quasicrystal that was created by the first nuclear explosion at Trinity Site, N.M., on July 16, 1945, could someday help scientists better understand illicit nuclear explosions and curb nuclear proliferation. Watch this video to learn more.

*Thin, stretchable biosensors could make surgery safer*

A research team from Los Alamos National Laboratory and Purdue University have developed bio-inks for biosensors that could help localize critical regions in tissues and organs during surgical operations.

### *Stress in Earth's crust determined without earthquake data*

Scientists at Los Alamos National Laboratory have developed a method to determine the orientation of mechanical stress in the Earth's crust without relying on data from earthquakes or drilling.

This method, which is less expensive than current approaches, could have broad applicability in geophysics and provide insight into continental regions lacking historical geologic information.

### *Bacteria, fungi interact far more often than previously thought*

In a novel, broad assessment of bacterial-fungal interactions, researchers using unique bioinformatics found that fungi host a remarkable diversity of bacteria, making bacterial-fungal interactions far more common and diverse than previously known.

### *Lightning in the water: Ultrafast X-ray provides new look at plasma discharge breakdown in water*

Lightning is fast, but how fast? A Laboratory collaboration recently turned to synchrotron X-rays for an answer. The story of the discovery of the connection between electricity and lightning is well known — in the 1700s, Benjamin Franklin, unaware of the danger of the electrical forces he was corraling, sent a key on a kite into the churn of a storm cloud. In the subsequent centuries, through experimentation and calculation, much has been learned about lightning, or plasma.

### *Guarding electrical power grids against hacker attacks*

Physicist Ray Newell and his team were testing how to protect electrical networks long before the hacking of Colonial Pipeline's operating computers. Newell presented his research on fiber-optics encryption, which is in use at Los Alamos Laboratory during a free, Lab-sponsored Frontiers in Science virtual talk in May.

### *Potential melanoma-fighting agent discovered on sea floor near Antarctica*

A Los Alamos scientist and his colleagues traced a naturally produced melanoma-fighting compound to a microbe that lives in an underwater species called an ascidian and known as a sea squirt. Scientist Patrick Chain noted the crucial detective work they performed to figure out which

organisms and the underlying molecular machines produce the potential anti-melanoma properties.

### *Decades of research brings quantum dots to brink of widespread use*

A new article in Science magazine gives an overview of almost three decades of research into colloidal quantum dots, assesses the technological progress for these nanometer-sized specs of semiconductor matter, and weighs the remaining challenges on the path to widespread commercialization for this promising technology with applications in everything from TVs to highly efficient sunlight collectors.

### *How microbiomes help secure the food chain*

Scientist Sanna Sevanto, in the Laboratory's Earth System Observations group, and her team are researching how microbial adjustments in soil can alter a plant's physiology. Could a plant be made to require less water by adding microbes? That's the question Sevanto is trying to answer. The team is currently studying the efficacy of two different microbiomes: one from the Crops Research Laboratory in Fort Collins, Colo., and the second from Los Alamos. Watch this video to learn more.

### *Translation software enables efficient DNA data storage*

In support of a major collaborative project to store massive amounts of data in DNA molecules, a Los Alamos National Laboratory–led team has developed a key enabling technology that translates digital binary files into the four-letter genetic alphabet needed for molecular storage.

### *Colloidal quantum dot lasers poised to come of age*

A new paper by authors from Los Alamos and Argonne national laboratories sums up the recent progress in colloidal-quantum-dot research and highlights the remaining challenges and opportunities in the rapidly developing field, which is poised to enable a wide array of new laser-based and LED-based technology applications.

To read more: <https://discover.lanl.gov/news/stories/1222-top-science-stories>

## The Cyber Defense Review: Addressing Critical Unlearned Lessons

Colonel Jeffrey M. Erickson



SPECIAL  
EDITION

VOLUME 7 ♦ NUMBER 1

WINTER 2022

# THE CYBER DEFENSE REVIEW

Welcome to a unique Special Edition of The Cyber Defense Review (CDR). For the last decade, those who have worked in the cyberspace domain will likely agree that some persistent issues and problems continue to be debated with no clear resolution. These include ideas and solutions that may have been identified but did not gain the necessary traction to achieve positive outcomes.

This issue focuses on those “Unlearned Lessons” from the last decade with the intent of encouraging action.

The variety of topics covered in the special edition are wide. In this issue, you will find articles on diplomacy, international relations, adversaries, alliances, emerging threats, economics, and beyond.

These are not just technical issues, but also societal and governmental challenges exacerbated through the dramatic nature of cyber technology.

Each article is kept intentionally short and to the point for maximum effect.

It is also worth pointing out that just because the US may not have learned these lessons, our adversaries may not be in the same situation.

Differences in government, priorities, and cultures may not be a hindrance to our adversaries. The “Unlearned Lessons” may have given our adversaries a first-mover advantage in the cyberspace domain, which further increases the need for us to consider, understand, and potentially act on these topics.

The special edition authors represent a diverse group of leaders from the cyberspace domain. They have all dedicated a significant portion of their professional careers wrestling with these challenging issues, and it is prudent that we all think about what they are saying.

When these authors speak, it is incumbent upon members of government, the military, academia, and industry to take the time and pay heed to their words.

A special thank you to Dr. Chris Demchak (Naval War College) and Prof. Francesca Spidalieri (University of Maryland) as the Guest Editors for crafting this critically important issue.

Their time and effort in making this issue a success and a must-read for the community are apparent throughout. We hope that continued dialogue with key leaders in the community will lead to decisive action.

As much as I look forward to future issues of the CDR, I hope that we do not have to see a “Lessons (Still) Unlearned from the Second Decade of Cyber Conflict” special edition ten years from now.

We can avoid ending up with that future issue by turning the page, considering the thoughtful points made by these authors, and then working to address these challenges within the larger community.

To read more:

[https://cyberdefensereview.army.mil/Portals/6/Documents/2022\\_winter/CDR\\_V7N1\\_WINTER\\_2022\\_Special\\_Edition\\_r7.pdf](https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/CDR_V7N1_WINTER_2022_Special_Edition_r7.pdf)

## Introducing Privacy Center



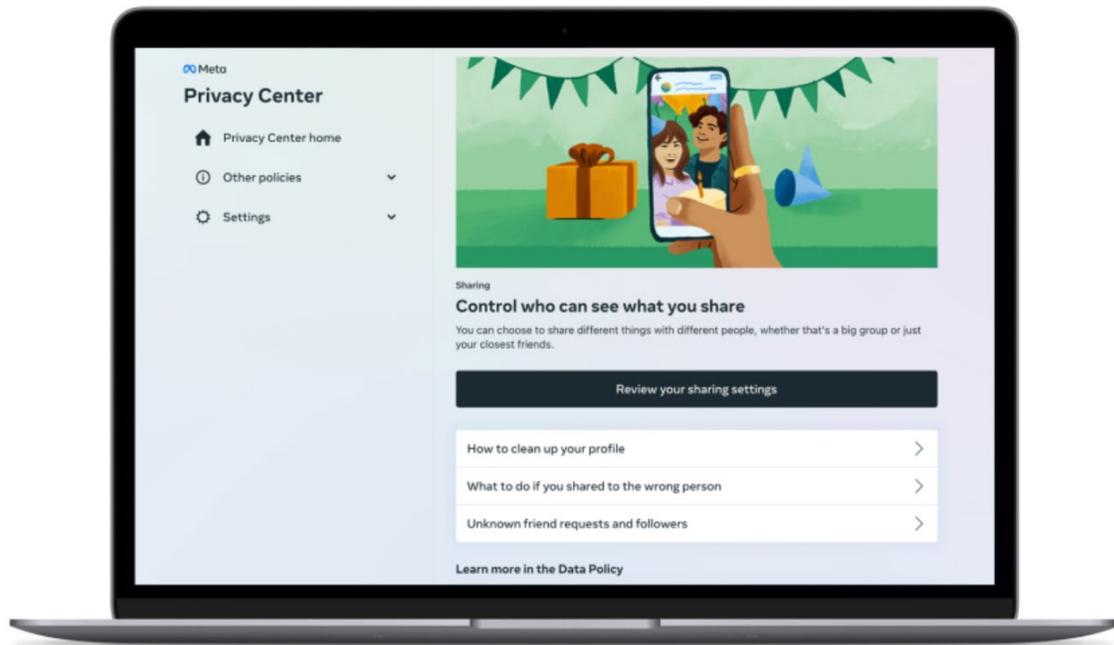
- We're introducing Privacy Center, a new place to learn more about our approach to privacy across our apps and technologies.
- Privacy Center provides helpful information about five common privacy topics: sharing, security, data collection, data use and ads.
- Privacy Center is now available to a limited number of people using Facebook on desktop in the US, and we plan to roll it out to more people and more of our apps in the coming months.

Today, we're introducing Privacy Center to educate people on their privacy options and make it easier to understand how we collect and use information. In Privacy Center, you can learn about our approach to privacy, read up on our Data Policy and learn how to use the many privacy and security controls that we offer.

To start, Privacy Center is now available to some people using Facebook on desktop, and we will roll it out to more people and apps in the coming months. We've built a number of privacy and security controls across our apps and technologies over the years, and our goal is for Privacy Center to serve as a hub for those controls and privacy education.

The current version of Privacy Center has five modules, each containing guides and controls related to a common privacy topic:

- **Security:** You can brush up on account security, set up tools like two-factor-authentication or learn more about how Meta fights data scraping.
- **Sharing:** You can visit this guide if you have questions about who sees what you post, or how you can clean up old posts on your profile using tools like Manage Activity.
- **Collection:** Learn about the different types of data that Meta collects, and how you can view that data through tools like Access Your Information.
- **Use:** Learn more about how and why we use data, and explore the controls we offer to manage how your information is used.
- **Ads:** Learn more about how your information is used to determine the ads you see, and make use of ad controls like Ad Preferences.



People who have access to this initial launch can find Privacy Center by navigating to Settings and Privacy on the desktop version of Facebook. As we expand Privacy Center, we will add more ways to access it in places where you may have privacy concerns.

We'll continue to update Privacy Center and add more modules and controls to help people understand our approach to privacy across our apps and technologies.

To read more: <https://about.fb.com/news/2022/01/introducing-privacy-center/>

## Cybercriminals Tampering with QR Codes to Steal Victim Funds



The FBI is issuing this announcement to raise awareness of malicious Quick Response (QR) codes. Cybercriminals are tampering with QR codes to redirect victims to malicious sites that steal login and financial information.

A QR code is a square barcode that a smartphone camera can scan and read to provide quick access to a website, to prompt the download of an application, and to direct payment to an intended recipient.

Businesses use QR codes legitimately to provide convenient contactless access and have used them more frequently during the COVID-19 pandemic.

However, cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use.

Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes.

A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information.

Access to this victim information gives the cybercriminal the ability to potentially steal funds through victim accounts.

Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location as well as personal and financial information.

The cybercriminal can leverage the stolen financial information to withdraw funds from victim accounts.

Businesses and individuals also use QR codes to facilitate payment. A business provides customers with a QR code directing them to a site where they can complete a payment transaction. However, a cybercriminal can replace the intended code with a tampered QR code and redirect the sender's payment for cybercriminal use.

While QR codes are not malicious in nature, it is important to practice caution when entering financial information as well as providing payment through a site navigated to through a QR code. Law enforcement cannot guarantee the recovery of lost funds after transfer.

*TIPS TO PROTECT YOURSELF:*

- Once you scan a QR code, check the URL to make sure it is the intended site and looks authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.
- Practice caution when entering login, personal, or financial information from a site navigated to from a QR code.
- If scanning a physical QR code, ensure the code has not been tampered with, such as with a sticker placed on top of the original code.
- Do not download an app from a QR code. Use your phone's app store for a safer download.
- If you receive an email stating a payment failed from a company you recently made a purchase with and the company states you can only complete the payment through a QR code, call the company to verify. Locate the company's phone number through a trusted site rather than a number provided in the email.
- Do not download a QR code scanner app. This increases your risk of downloading malware onto your device. Most phones have a built-in scanner through the camera app.
- If you receive a QR code that you believe to be from someone you know, reach out to them through a known number or address to verify that the code is from them.
- Avoid making payments through a site navigated to from a QR code. Instead, manually enter a known and trusted URL to complete the payment.

*Revisiting an important speech*

## Dynamic Regulation for a Dynamic Society

Chair Gary Gensler, before the Exchequer Club of Washington, D.C.



Thank you for the kind introduction. As is customary, I'd like to note that my views are my own, and I'm not speaking on behalf of the Commission or SEC staff.

I'd like to share with you all that we lost an SEC alum, Robert Birnbaum, this past December. Though I didn't get to know Bob personally, he accomplished a lot in his remarkable life. After leaving the SEC, he went on to lead the New York Stock Exchange.

While at our agency, though, Bob contributed to a seminal report called the Special Study. This report was published in 1963 — exactly 30 years after Franklin Delano Roosevelt and Congress came together, in the depths of the Great Depression, to think about how our capital markets could work better for the American public.

The 1963 report described our securities laws as “a proven legislative achievement.” And yet, the staff wrote, “no regulation can be static in a dynamic society.” They continued, “unanticipated changes in the markets and the broader public participation should be accompanied by corresponding investor protection.”

Indeed, a lot had changed in the capital markets over the previous 30 years. Based upon that report, Congress would go on to amend the securities laws over the next dozen years, bringing SEC oversight to over-the-counter markets, facilitating a national market system, and banning fixed commissions.

Over the past several decades, our markets have continued to evolve in an even more dramatic way. Policymakers have continued to change our laws and our regulations in response.

We are blessed with the largest, most sophisticated, and most innovative capital markets in the world. The U.S. capital markets represent about 40 percent of the globe's capital markets. This exceeds even our impact on the world's gross domestic product, where we hold a 24 percent share.

But, as Bob's team noted, we cannot take this for granted; "no regulation can be static in a dynamic society." In 2022, nearly six decades after the publication of the Special Study, that core idea still rings so true.

Today, I'd like to share with you a couple of guiding principles I think about when it comes to making regulations "dynamic" in shaping the SEC's agenda for 2022:

- First, continuing to drive efficiency in our capital markets
- Second, modernizing our rules for today's economy and technologies

### *Driving Efficiency in Our Capital Markets*

Let me start with efficiency.

Why does efficiency matter?

Efficiency in capital markets is about lowering costs of intermediation for those who use capital — issuers — and those who own capital — investors. This fits directly into our mission, which is to protect investors, facilitate capital formation, and maintain that which sits between investors and issuers: fair, orderly, and efficient markets.

Today, the financial sector, including the capital markets, banking, and insurance, represents about 8 percent of America's economy. In 1963, when the Special Study was published, the sector had a 3.5 percent share. While a lot has changed in our economy since then, I think the SEC still has a role to play to help drive greater efficiency here.

Further, one study found that the costs of financial intermediation over time were as high in 2014 as they were in 1900. The scholar found this "puzzling," as advances in technology "should lower the physical transaction costs of buying, pooling and holding financial assets."

To promote efficiency, over the decades Congress has given us a number of tools to foster competition and transparency. Congress made significant amendments to our statutes in 1975, partly in response to the Special Study. In the very first line of that bill, it says they were "amend[ing] the Securities Exchange Act of 1934 to remove barriers to competition." That word, "competition," appears 20 times in the text.

Congress returned to this idea of competition again in 1996. In rulemaking, Congress said, the Commission must consider efficiency, competition, and capital formation, in addition to investor protection and the public interest. Those are tools that, if used correctly, can lead to greater productivity and lower economic rents.

Hence, I've directed our staff to make recommendations up and down the capital markets about how we can drive towards greater efficiency through competition and transparency. This includes various sectors: the \$50 trillion equity markets; our \$23 trillion Treasury markets, whose "issuers" are the American public and the Department of the Treasury; and other aspects of the \$25 trillion non-Treasury fixed income markets. It also includes the fund management area.

Let's take a quick look at one area of fund management in particular: private equity and hedge funds. These funds hold about \$17 trillion in gross assets under management. While we don't know the exact costs of doing business in this sector, there may be around \$250 billion in fees and expenses each year.

If we can use our authorities to bring greater transparency and competition into that market, that helps portfolio companies on the one hand, and the pensions and endowments that are investing in that space on the other. Similarly, if we can drive efficiencies across other key sectors of the capital markets, that too would help issuers and investors.

### *Modernizing Our Rule Set for Today's Economy and Technologies*

Next, I'd like to turn to updating our rule set for today's economy and technologies.

Markets and business models have long evolved in response to new technologies; as Bob Birnbaum's team noted, they are "dynamic." I believe that innovation can bring greater access, efficiency, and innovation to our capital markets, as well as economic growth.

Our central question is this, though: When new technologies come along and change the face of finance, how do we continue to achieve our core public policy goals?

Here again, Bob's team gives us some insights. By 1963, the development of communications systems after World War II had made it easier for broker-dealers to transact directly. One of the main things Bob and his team were looking at was this over-the-counter market.

They wrote, "In the 'old days,' one of the major tasks was to locate a market—a task often performed by mail. Now...markets for most securities can be located almost instantaneously and transactions consummated within a matter of seconds."

If that was true of 1963, it is true by several orders of magnitude today. "A matter of seconds" can be an eternity in today's markets!

What does this mean for the 2020s? Some will jump to crypto, of course. I'll leave that for your questions. Before that, let me raise a couple of other categories as well:

To me, the most dramatic change to our markets is the use of predictive data analytics and artificial intelligence. Predictive data analytics, including machine learning, are increasingly being adopted in finance — from trading, to asset management, to risk management. Though we're still in the early stages of these developments, I think the transformation we're living through now could be every bit as big as the internet was in the 1990s.

While these developments can increase access and choice, they also raise important public policy considerations, including conflicts of interest, bias, and systemic risks.

Innovation doesn't come just from updating software and hardware; it also comes from the manner in which products are offered. One example today is around how many issuers have sought alternative ways to access public markets through special purpose acquisition companies (SPACs) and direct listings.

Beyond the innovations and technologies, our economy is changing in other ways. Today, investors are demanding additional information from companies beyond what they've sought historically, with respect to climate risk, human capital, and cybersecurity risk. Our core bargain from the 1930s is that investors get to decide which risks to take, as long as public companies provide full and fair disclosure and are truthful in those disclosures.

All of this is exciting. Innovation and evolution keep our markets the most robust in the world. Our role at the SEC, though, is to help ensure that we still achieve our public policy goals as mandated in our mission.

Again, “no regulation can be static in a dynamic society.”

### *Looking Forward*

Before I conclude, a few thoughts on 2022.

We made good progress in 2021, finalizing a handful of rules and proposing many others. We have much more to come on the SEC's Agency Rule List.

I'm often asked to prioritize the remaining items on our rulemaking agenda. When will we vote on what?

At their core, those questions are more about sequencing than prioritization. Staff is working hard on proposals. When they and my fellow Commissioners think they're ready, we'll put them out for public comment and, when appropriate, finalize items.

The process is intentionally flexible; it's about getting proposals right, based upon the economic analysis and our legal authorities, and learning from public feedback. I encourage you all to weigh in on those proposals when they're available. We also have an Open Commission Meeting next week, so stay tuned for that.

I just want to say something about this incredible agency.

Since joining the SEC last spring, I have been struck by the sheer breadth and scope of the agency's work. We oversee every corner of the \$100-trillion capital markets — all of its sectors, from equity markets to municipal bonds, and functions, from accounting and auditing to disclosure to fund management. Nearly half of our agency works as cops on the beat in our terrific Divisions of Examinations and Enforcement. Behind the scenes, so many folks are making our operations hum. All this, despite the challenges presented by this pandemic.

They make me proud to be their colleague; they do right by the American public every day. I know they made Bob Birnbaum proud as well. I am grateful to call them teammates and look forward to continue collaborating with them in 2022.

Thank you and I'm happy to answer any questions.

## Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of an interpretative document;
- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

## Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: [https://www.sarbanes-oxley-association.com/How\\_to\\_become\\_member.htm](https://www.sarbanes-oxley-association.com/How_to_become_member.htm)

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: [https://www.sarbanes-oxley-association.com/Reading\\_Room.htm](https://www.sarbanes-oxley-association.com/Reading_Room.htm)

3. Training and Certification - You may visit: [https://www.sarbanes-oxley-association.com/Distance\\_Learning\\_and\\_Certification.htm](https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm)

[https://www.sarbanes-oxley-association.com/CJSOXE\\_Distance\\_Learning\\_and\\_Certification.htm](https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm)

For instructor-led training, you may contact us. We tailor all programs to meet specific requirements.