GFMI
GLOBAL FINANCIAL MARKETS INSTITUTE

Article **2026**

The Finance Industry and Article Three of the North Atlantic Treaty: Coordinating Evolving and Converging Threats

by Alma Angotti and William Jannace

The article expresses the personal views of the authors and does not necessarily reflect the views of any organizations with which either is affiliated.

The authors wish to acknowledge the contributions of Ashleigh Szydlowski and Mae Signorello.

The Finance Industry and Article Three of the North Atlantic Treaty: Coordinating Evolving and Converging Threats

Article 5[1]

At the 2016 Warsaw Summit, the NATO Alliance reaffirmed that a cyber attack against any member state can trigger the Article 5 collective defense clause, reinforcing that cyberspace is an operational domain, just like land, air, and sea. NATO declared that cyber attacks that commit denial or destruction effects could meet the threshold of an armed attack and, depending on the severity, prompt a coordinated response.[2] In a world of evolving threats, strategic competition is less focused on the seizure of geographic ground and more on the manipulation of systems that states rely on to function. Strategic terrain is no longer primarily geographic, but now includes infrastructure, institutions, markets, and information systems that influence a state's ability to govern, mobilize, and compete. Disruptive cyber attacks manifest across borders without physically crossing them. Such attacks may trigger Article 5 without involving a kinetic attack on the soil of a NATO member. Such attacks continue on the networks and infrastructure of the United States[3] and its NATO allies.

Article 3 and Resiliency[4]

The issue of whether NATO can respond to such attacks by invoking Article 5[5] may depend upon utilizing Article 3. As the NATO Charter notes in Article 3, each member country needs to be resilient to resist and recover from a major shock such as a natural disaster, failure of critical infrastructure, or a hybrid or armed attack.[6]

Article 3 complements the collective defense clause set out in Article 5. The individual commitment of each NATO member to maintain and strengthen its resilience reduces the vulnerability of NATO. When Allies are well prepared, they are less vulnerable or less likely to be attacked, making NATO stronger.[7]

Today's security environment is unpredictable. Attacks can come from state and non-state actors, involving cyber attacks or hybrid warfare, which blur the lines between conventional and unconventional forms of conflict.[8] The challenge of adapting and responding to these types of threats is exacerbated by trends that have transformed the security environment in the EU. For example, falling defense budgets since the end of the Cold War had gradually increased the overall reliance on civil and commercial assets and capabilities.[9] This trend, however, has recently changed following the Russian invasion of Ukraine.[10] Modern warfare has shifted from solely the battlefield to infrastructure, markets, and information that sustain a nation. In this new paradigm, strategic terrain is defined by the manipulation of global supply chains and regulatory frameworks, allowing adversaries and other malign actors to exert influence long before a kinetic

action is undertaken. Understanding these new and evolving systemic vulnerabilities is now the only way to prevent strategic surprise in an era where power is projected through technology and economic ties rather than bullets and borders.[11]

Evolving Nature of the Cyber Threat

Coordinated Nation-State Attacks

In a report entitled, "Cybersecurity: Selected Cyberattacks, 2012-2025," many members in Congress expressed concern over the growth in frequency, type, and impact of cyber incidents against and in the United States. The report also described that cyberattacks against entities in the United States were attributed to actors operating on behalf of a nation-state and to criminal actors seeking personal gain.[12] Further, the report highlighted cyberspace as an area of strategic concern, with People's Republic of China (China, or PRC), the Russian Federation (Russia), the Democratic People's Republic of Korea (North Korea), and the Islamic Republic of Iran (Iran) called out by the report as the leading threat actors.[13]

This threat continues to evolve, as PRC cyberspace campaigns such as Volt Typhoon[14] and Salt Typhoon are not merely routine espionage. Such operations reflect a PRC-coordinated effort to pre-position access across vital systems, enabling potential disruption of military logistics and civilian infrastructure,[15] which supports financial industry mission critical systems,[16] in the early phases of a crisis. Some argue that U.S. cyber deterrence has failed not for lack of capability, but for lack of resolve and strategic coherence, as cyber operations exploit national security asymmetry: below the level of kinetic activity that would trigger a decisive U.S. response. As a result, adversaries have been able to operate below the threshold of response while steadily expanding their cyberspace foothold in the U.S., which calls for a whole-of-government approach that treats cyber intrusions into critical infrastructure as intolerable national security threats. It emphasizes the need for visible, coordinated responses—led at the presidential level—to restore credible deterrence and prevent adversaries from exploiting persistent access within U.S. systems.[17]

Parallel Tracks Converging

United States Cyber Command

U.S. Cyber Command (USCYBERCOM), the nation's unified combatant command for the cyberspace domain, was established in 2010. USCYBERCOM is a military command that operates globally in real time against capable adversaries. It is composed of military, intelligence, and information technology capabilities, with its mission to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.[18]

U.S. Cyber Command also executes two-way information-sharing agreements with partners from across the public and private sectors. These agreements are designed to enhance and expand trust and dialog between its partners and USCYBERCOM. Once an agreement is in place, members of the program work with USCYBERCOM's partners to facilitate sharing of critical information across multiple mediums, all to defend the nation against foreign adversary threats in and through cyberspace. U.S. Cyber Command also collaborates with academic institutions to engage the future workforce, increase cyber applied research and innovation, expand cyber-focused analytic partnerships, and enrich strategic cyber dialogue.[19]

In 2025, the Department of War (DoW) established CYBERCOM 2.0, a revised Cyber Force Generation Model, to enhance its ability to better respond decisively against evolving threats in the cyber domain. In its announcement, the DoW noted that since USCYBERCOM was established it has relied on traditional military services' man, train, and equip models to source its cyber forces. While appropriate for other warfare domains, these models have not met the unique requirements necessary to fight and win in the cyber domain. CYBERCOM 2.0 is intended to produce a cyber force capable, according to the press release, of "defeating threats posed by China in cyberspace and delivering asymmetric options otherwise unavailable to national decision makers and joint force commanders."[20]

Artificial Intelligence as a Force Multiplier for Cybersecurity Risks

In 2024, the U.S. Department of the Treasury (Treasury) issued a report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector. The Treasury report identified significant opportunities and challenges that AI presents to the security and resiliency of the financial services industry. It outlined, among others, certain steps to address immediate AI-related operational risk, cybersecurity, and fraud challenges:[21]

> (1) There is a widening gap between large and small financial institutions (FIs). Larger FIs may develop in-house AI systems or have the resources to purchase the necessary software. Smaller FIs may lack large budgets for new technology or the internal data science resources required to develop and train large language models.
>
> (2) As more FIs deploy AI, some institutions may lack appropriate data for training models. This gap is significant in fraud prevention, where there is insufficient data sharing among firms.
>
> (3) While FIs and regulators are collaborating on how best to resolve oversight concerns together, different financial-sector regulators at the state and federal levels, and internationally, may cause regulatory fragmentation if the regulatory frameworks for AI diverge.

(4) The National Institute of Standards and Technology (NIST) AI Risk Management Framework could be expanded and tailored to include more applicable content on AI governance and risk management related to the financial services sector.[22]

Claude Mythos Review

In April 2026, Anthropic announced information on its Claude Mythos Preview, a new general purpose language model that is very autonomous and capable at computer security tasks, software coding, and complex reasoning objectives.[23] It was also reported that Treasury Secretary Scott Bessent and former Federal Reserve (Fed) Chair Jerome Powell summoned leaders of several financial services firms to a meeting on Mythos' capabilities to detect potential cybersecurity weaknesses and the potential risks that could arise from those capabilities.[24] JPMorgan, Morgan Stanley, Goldman Sachs, Citi, and Bank of America have advised that that they have access to Mythos.[25] In June 2026, Anthropic announced that it had expanded Project Glasswing to include 150 new organizations.[26]

Financial Services Industry and Article Three of NATO

Post 9/11, the financial services industry elevated the importance of business continuity and contingency planning in the form of mandated regulation. For example, FINRA now requires member firms to create and maintain written business continuity plans (BCPs) relating to an emergency or significant business disruption. Rule 4370[27]—FINRA's emergency preparedness rule—delineates required BCP procedures. A firm's BCP must be appropriate to the scale and scope of its business.[28] BCP procedures must be reasonably designed so the FINRA member firm can meet its existing obligations to customers. A member firm must disclose to its customers how its BCP addresses the possibility of a significant business disruption and how the firm plans to respond to events of varying scopes. This BCP disclosure must be made in writing to customers when they open their account, posted on the firm's website if they maintain one, and mailed to customers upon request. The BCP also must be made available promptly to FINRA if requested.[29]

As discussed in more detail below, the Securities Industry and Financial Markets Association (SIFMA) plays a vital role in coordinating BCP and contingency planning for clearing and introducing firms to ensure operational resiliency across U.S. capital markets. Through annual industry-wide testing,[30] emergency command center coordination, and dedicated Treasury clearing workstreams, SIFMA helps firms prepare for significant disruptions, including cyber threats, severe weather, and market IT failures.[31]

Regulation S-P, SEC Guidance on BCP and Regulation SCI

Regulation S-P

Regulation S-P requires registered broker-dealers, investment companies, and investment advisers to establish written policies and procedures that address administrative, technical, and physical

safeguards for the protection of customer records and information.[32] Regulation S-P also requires covered institutions to (1) adopt an incident response program and (2) notify affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[33] SEC rules require disclose of material aspects of cybersecurity incidents they experience (such as nature, scope, timing, material impact) within four business days after the firm determines the incident is material; and material information regarding their cybersecurity risk management, strategy and governance on an annual basis.[34] Liability extends to firms when utilizing third party vendors for compliance with these requirements.[35]

BCP Guidance

Post 9/11, the SEC articulated its expectations for each Self-Regulatory Organization Market (SRO Market) and Electronic Communications Networks (ECNs) to apply the following principles in its BCP planning:[36]

1. Each SRO Market and ECN should have a BCP that anticipates the resumption of trading in the securities traded by that market no later than the next business day following a wide-scale disruption. The resilience of the SRO Market or ECN prescribed by such BCP should reflect the extent of alternative trading venues for the securities traded by that market, including the number of sole listings on the market, the market share of the market, and the number of sole members or subscribers of the market. BCPs may focus on strengthening the SRO Market's or ECN's own resilience, on backup arrangements with other markets, or both.

2. Assuring resumption of trading activities by a market by the next business day generally requires geographic diversity between primary and backup sites. To be fully resilient, backup sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, and electric power) used by the primary site, and the operation of such sites should not be impaired by a wide-scale evacuation of or the inaccessibility of staff that service the primary site.

3. SRO Markets also should assure full resilience of shared information systems, such as the consolidated market data generated for the equity and options markets.[37]

4. The effectiveness of back-up arrangements in recovering from a wide-scale disruption should be confirmed through testing.[38]

Regulation SCI

After the above SEC guidance, the industry evolved whereby stock exchanges demutualized and became publicly traded and expanded resources to capture market share. Issues with respect to technological glitches raised concerns about the adequacy of resourcing technology and resiliency.[39] Subsequently the SEC promulgated Regulation Systems Compliance and Integrity

(Regulation SCI) under the Securities Exchange Act of 1934 (Exchange Act) which applies to certain self-regulatory organizations (including registered clearing agencies), alternative trading systems (ATSs), plan processors, and exempt clearing agencies (collectively SCI entities),[40] and will require these SCI entities to comply with requirements with respect to the automated systems central to the performance of their regulated activities.[41]

The Impact of Shortened Settlement Cycles on BCPs and Regulation SCI

As the industry moved towards a T+1 settlement cycle and 23/5 trading resiliency is even more vital than ever. It was recently noted that financial services firms are embedding resilience into core operating models rather than treating it as a standalone BCP function, with the move to T+1 settlement accelerating that transition. Specifically, the transition to T+1 settlement has changed how firms respond to operational disruption in a compressed timeframe.[42]

The push towards 23/5 trading and extended market hours reduces operational windows, forcing firms to redesign workflows and controls over compressed time periods. For example, under T+2, firms had about 19.5 hours after market close to complete trade affirmation and clearing preparation. Under T+1, that window has been reduced to approximately five hours. To address these issues firms are increasingly adopting cross-functional resilience models that bring together operational risk, cybersecurity, legal, communications, and business teams earlier in decision-making.[43]

FINRA's and SIFMA's Roles in Operational Resiliency and Cybersecurity

FINRA

FINRA Rule 4380 (Mandatory Participation in FINRA BC/DR Testing Under Regulation SCI) provides, in part, that in accordance with Rule 1004 of SEC Regulation SCI, FINRA will designate members that will be required to participate in FINRA's periodic, scheduled testing of its business continuity and disaster recovery (BC/DR) plan. FINRA will do so according to established criteria that are designed to ensure participation by those members that FINRA reasonably determines are, taken as a whole, the minimum necessary for the maintenance of fair and orderly markets in the event of the activation of its BC/DR plan. FINRA's criteria will consider volume of activity on a FINRA market system over a specified period. FINRA will communicate to members its criteria for designation under this Rule, and any changes to such criteria, on a prospective basis by Regulatory Notice.[44]

Allocating Responsibilities and Industry Cybersecurity Resiliency

Carrying and clearing agreements are contractual arrangements reviewed and approved by FINRA where a carrying firm broker-dealer (a clearing firm) provides custody, trade execution, and back-office services for an introducing firm broker-dealer (smaller broker-dealers).[45] These arrangements are governed by FINRA Rule 4311,[46] which allows these agreements permitting the

introducing firm to focus on client relationships while the clearing firm manages regulatory, custodial, and operational tasks.

FINRA's Cyber and Analytics Unit (CAU) has highlighted cybersecurity risks at third-party providers impacting its member firms. Since 2023, it has observed an increase in cyber attacks and outages at third-party providers used by its member firms.[47] The financial industry's reliance on third-party providers to support several key systems or covered functions (such as clearance and settlement pursuant to carrying/clearing arrangements) exacerbates the risk to member firms.[48] An attempted cyber attack or an outage at a third-party provider could potentially impact a large number of member firms.[49] To address these concerns, FINRA has advised its member firms to report to their FINRA Risk Monitoring Analysts changes to third-party providers that support key systems or any cybersecurity events at third-party providers.[50]

FINRA Cybersecurity Practices

FINRA evaluates its member firms' approaches to cybersecurity risk management through reviews of their controls in areas including technology governance, risk assessment, technical controls, access management, incident response, vendor management, data loss prevention, system change management, branch controls, and staff training. Through these reviews, FINRA assesses a member firm's ability to protect the confidentiality, integrity, and availability of sensitive customer information.[51]

FINRA also hosts Cyber Workshops and Tabletop Exercises to help its member firms strengthen their cyber readiness, reinforce internal controls, and better understand expectations around safeguarding customer data and maintaining operational resilience.[52] FINRA's Cyber and Operational Resilience provides intelligence, training, and practical guidance to help member firms identify risks, respond effectively, and build sustainable resilience.[53]

Financial Intelligence Fusion Center

FINRA launched its Financial Intelligence Fusion Center (FIFC), a secure portal for FINRA and its member firms to share intelligence about cybersecurity and fraud threats and coordinate responses. The FIFC will collect, analyze, and disseminate threat intelligence to bolster its member firms' awareness and ability to quickly respond to these threats. The FIFC will also leverage FINRA's existing partnerships, enabling input from other governmental and private sector partners.[54]

SIFMA

Business Continuity

As noted above, SIFMA coordinates an Industry-Wide Business Continuity Test[55] to evaluate financial services firms' ability to operate under stress. It involves all major exchanges, utilities,

and market participants, with the test including transactions across equities, options, futures, fixed income, settlement, payments, Treasury auctions, and market data.[56] It runs in coordination with the Futures Industry Association and every other year with the Investment Industry Regulatory Organization of Canada (IIROC).[57]

Cybersecurity

SIFMA notes that the securities industry supports the NIST Cybersecurity Framework[58] as a foundation for global, risk-based standards, and that the Cyber Risk Institute's Financial Services Cybersecurity Profile[59] serves as a benchmark for compliance and supervisory alignment across the sector. In addition, a combined resource from SIFMA and the Financial Services Sector Coordinating Council (FSSCC) provides a five-step mitigation framework covering: Assess, Remediate, Assure, Reconnect, and Recover, which is intended to support and inform a technical view of reconnection as well as broader resilience planning.[60]

Further, SIFMA's Quantum Dawn[61] exercises bring together financial institutions, market utilities, and government partners to simulate systemic cyber incidents and improve coordination, communication, and response capabilities. They are among the most comprehensive cybersecurity readiness programs in the financial services industry.[62] In March 2026, SIFMA issued an after-action report from its Quantum Dawn VIII resilience exercise conducted in November 2025.[63] The exercise simulated multiple distinct events which simultaneously impacted the sector, including a Category 5 hurricane, a transatlantic cable cut, a Financial Market Infrastructure outage, and a zero-day cybersecurity attack attributed to a state actor.[64]

SIFMA noted that overall, the exercise demonstrated the financial services sector's confidence in its ability to respond to disruption, and importance of a robust partnership between the industry and government based on information sharing. SIFMA also noted that no individual stakeholder, whether it be the government or any individual firm, has the resources to protect markets from the full panoply of threats on their own, nor do incidents necessarily restrict themselves to one geographic region.[65]

Global Initiatives

Financial Stability[66]

In 2019, the Carnegie Endowment for International Peace's Cyber Policy Initiative launched a project and issued a report entitled, "International Strategy to Better Protect the Financial System Against Cyber Threats."[67] The Cyber Policy Initiative built on existing efforts, identified gaps, and outlined a more comprehensive approach to maximize the impact of existing activities, strengthen the connective tissue between them, and propose next steps. This includes outlining how emerging best practices and lessons learned could be internationalized and implemented.[68]

BIS Cyber Resilience Coordination Centre

The Bank for International Settlements (BIS) Cyber Resilience Coordination Centre (CRCC) helps to strengthen the collective cyber resilience of central banks by providing a structured approach to knowledge-sharing, collaboration, and operational readiness. The CRCC carries out its mandate as one of the BIS' key entities to support the central bank community by delivering cyber resilience services in three main activity areas: knowledge-sharing, collaboration, and operational readiness.[69]

The G7 Cyber Expert Group

The Cybersecurity and Infrastructure Security Agency and the Group of Seven (G7)[70] issued joint guidance, Software Bill of Materials for AI – Minimum Elements, to help public and private sector stakeholders improve transparency in their AI systems and supply chains.[71]

Global Financial Markets Association

SIFMA collaborates with the Global Financial Markets Association and other international organizations[72] to advance consistent operational resilience standards across jurisdictions. For example, the Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry, was developed with global partners to promote consistent expectations and continuous improvement in cyber defense.[73]

The European Supervisory Authorities

The European Supervisory Authorities[74] published their first annual overview of major Information Communication Technology (ICT) related incidents to the EU financial sector, pursuant to a reporting mechanism established by the Digital Operational Resilience Act.[75] According to this report, ICT risks are increasingly borderless and interconnected, and that the recent evolution of very capable AI-driven tools should encourage financial entities to strengthen cybersecurity measures to maintain their resilience going forward.[76] The report further noted that approximately one third of the 3,383 major incidents reported by financial entities in the EU had a cross-border impact, highlighting the growing interconnectedness through shared infrastructures and services.[77] While only noting that 10 percent of the reported incidents were related to cybersecurity, it stressed that financial entities maintain the highest cybersecurity standards to keep pace with the potential use of highly capable AI-driven tools.[78]

The Convergence[79]

Financial Stability Oversight Council

The Financial Stability Oversight Council (FSOC) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act and is charged with three purposes:

1. To identify risks to the financial stability of the U.S. that could arise from the material financial distress or failure, or ongoing activities, of large, interconnected bank holding companies or nonbank financial companies, or that could arise outside the financial services marketplace.

2. To promote market discipline by eliminating expectations on the part of shareholders, creditors, and counterparties of such companies that the U.S. government will shield them from losses in the event of failure.

3. To respond to emerging threats to the stability of the U.S. financial system.

The 2025 FSOC Report notes that the cyber threat landscape is evolving with nation-state actors and sophisticated criminal groups continuing to target financial institutions, as they are lucrative targets because they manage substantial funds, hold sensitive customer data, and can be impacted by operational disruptions. It further noted that although cyber incidents have not resulted in a significant systemic event for the U.S. financial services sector to date, they could pose risks to financial stability given the high complexity and interconnectedness of global financial institutions and their systems. The potential consequences of cyber incidents include large-scale service disruptions, challenges with accessing liquidity, compromised data, and a loss of confidence in institutions, markets, and the global financial system.[80]

March 2026 Cyber Strategy for America

President Trump's March 2026 "Cyber Strategy for America" notes that American citizens, companies, and U.S. allies should not have to fend off sophisticated military, intelligence, and criminal adversaries in cyberspace alone. The U.S., it pledges, will utilize the full suite of its defensive and offensive cyber operations, and will unleash the private sector by creating incentives to identify and disrupt adversary networks and scale its national capabilities. The U.S. must detect, confront, and defeat cyber adversaries before they breach U.S. networks and systems. The U.S. will erode their capacity and capabilities and use all instruments of national power to raise the costs for their aggression. The U.S. will establish a new level of relationship between the public and private sectors to defend America in peace and war. The U.S. will eliminate roadblocks that prevent industry, academia, government, and the military from aligning incentives and building a highly skilled cyber workforce.[81]

Promoting Advanced Artificial Intelligence Innovation and Security

President Trump signed an executive order directing federal agencies to promote advanced AI innovation while strengthening cybersecurity defenses across government and critical infrastructure. The order calls for an AI cybersecurity clearinghouse, expanded access to AI-enabled defensive tools, and a voluntary framework for developers to give the federal government early access to certain frontier models before broader release. The effort is intended

to support secure AI deployment, protect U.S. intellectual property, and harden public and private systems against emerging threats.[82]

The Financial Sector Risk Management Plan

The Financial Sector Risk Management Plan (The 2025 Plan), prepared by the Treasury in collaboration with the FSSCC,[83] identifies the approaches to be taken in addressing and mitigating the most significant risks facing the U.S. financial services industry.[84] The 2025 Plan aligns with U.S. national security priorities, including directives from the U.S. Department of Homeland Security. It was reviewed by the Financial and Banking Information Infrastructure Committee (FBIIC)[85] as the government coordinating council for the financial services sector.[86]

The 2025 Plan responds to the evolving risk environment, particularly the increasing importance of cybersecurity to the sector, and reflects progress made on building a collaborative public-private partnership since the release of the 2015 Financial Sector-Specific Plan.[87]

The 2025 Plan describes the components, services offered, and key dependencies and interdependencies of the financial sector, and outlines priority risks including, among others:[88]

1. Geopolitical conflict poses risk to the financial services sector because of the international footprint of U.S. financial sector firms and the willingness of hostile nations to target U.S. financial sector firms.

2. Emerging technologies pose risks because they have the potential to impact the financial services sector in unpredictable ways.

3. Cloud concentration poses risk because of increasing reliance of the financial services sector on a limited number of cloud service providers for a variety of information technology services.

4. Supply chains pose risk because of the software and hardware that enable information.

5. Financial market operations pose operational risk to the sector because reliance on critical utility functions may create single points of failure that could disrupt financial sector operations in the event of an outage.

6. Critical infrastructure dependencies pose risk because financial institutions depend on other sectors for key services like IT, communications, energy, and emergency services.

The 2025 Plan outlines six “lines of effort” aimed at reducing the consequences of adverse incidents:

1. Promote Adoption of Voluntary Minimum Security and Resilience Best Practices. FIs and government agencies work together to promote the use of common approaches and best practices for enhancing security and resilience to prevent incidents from occurring whenever possible and minimize the impacts of incidents that do occur.

2. Develop and Promote Common Collective Security Solutions. Ensuring that information, such as attack indicators, are expeditiously delivered in a usable format to those who need it, particularly cybersecurity information sharing where incidents can unfold instantaneously.

3. Enhance Incident Response and Recovery. The sector maintains and enhances processes for facilitating a whole-of-sector response to incidents and for coordinating these response efforts among firms, security service providers, regulators, law enforcement, executive branch agencies, and international partners.

4. Manage the Integration of Artificial Intelligence. In response to Treasury's report, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector," CEG the Treasury, the FBIIC, and the FSSCC initiated workstreams to address the challenges identified in the report to help FIs mitigate operational risk, cybersecurity, and fraud issues associated with the use of AI technologies.

5. Advance Resiliency of Cloud Adoption. Treasury's report, "The Financial Services Sector's Adoption of Cloud Services," described the current state of cloud adoption in the sector, including potential benefits and challenges associated with increased adoption.

6. Prepare for Quantum Computing.[89] Under the leadership of Treasury and the Board of Governors of the Federal Reserve System, the G7 Cyber Experts Group (CEG), with representation from financial regulators and industry, is exploring the nexus between emerging technologies and security, including quantum computing.

"The Best Defense is a Good Offense"

The quote has been ascribed to various sports and historical figures, but in the continuing evolution of hybrid-gray zone warfare, the growing threats the financial services industry faces, it is a path forward for industry to combat evolving cyber threats.[90]

The U.S. has reentered a period in which economic vitality and stability is central to national security, with competition running through supply chains, energy systems, financial infrastructure, communications networks, and technology ecosystems. Private sector firms are both instruments and arenas of that competition, operating directly on the front lines. They are not immune and indifferent to such risk, but they lack the holistic national security perspective and resources to respond individually. Both the industry and the government should recognize the strategic risks confronting the U.S. and the operational risks for U.S. financial services firms, as they are increasingly interconnected.[91] To address this evolving and growing threat, a whole-of-

government approach[92] may be needed that treats cyber intrusions into critical infrastructure as unacceptable national security threats, requiring coordinated responses to restore deterrence and prevent adversaries from exploiting persistent access within U.S. systems.[93] We may not be at a point of having financial services firms invoke a coordinated Article 5 type response to individual cyber attacks. However, as the resiliency of the industry and critical U.S. infrastructure continues to be tested, evolving options, such as using circuit breakers for Application Program Interface-initiated transactions,[94] may be necessary in an increasingly amorphous world of hybrid-gray zone warfare.

About the Author: Alma Angotti

Alma Angotti is a recognized expert in financial crime compliance and economic sanctions with more than 30 years of experience in both regulatory enforcement and global consulting. Alma has held senior enforcement roles at the U.S. Securities and Exchange Commission (SEC), the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the Financial Industry Regulatory Authority (FINRA). She brings deep subject matter expertise in regulatory compliance, including Bank Secrecy Act/Anti-money Laundering (BSA/AML), sanctions, and counter-terrorist financing (CFT).

At FTI Consulting, Alma advises clients on compliance risk assessments, remediation strategies, enforcement preparedness and regulatory investigations. Her clients include global and mid-sized financial institutions; global fintech firms; digital assets and payments institutions; stablecoins and cryptocurrency platforms; broker-dealers; hedge funds; casinos; and multinational corporations.

Alma serves on the advisory boards of the Global Digital Asset and Cryptocurrency Association and the Digital Dollar Project. At FinCEN and FINRA, she designed and led the AML enforcement programs and regularly trains regulators and government officials worldwide on AML and financial crime compliance matters. Additionally, she has been approved to be an independent compliance monitor by federal and state regulatory agencies, including the SEC, the Office of the Comptroller of the Currency (OCC) and the New York State Department of Financial Services (NYDFS).

About the Author: William Jannace

William Jannace is an Associate Professor at the Dwight D. Eisenhower School for National Security and Resource Strategy/National Defense University, where he teaches courses on economics and finance and national security. He has also served as an expert witness for The Bates Group on securities litigation matters. He is also an adjunct professor/lecturer at Fordham School of Law, Global Financial Markets Institute, and Metropolitan College, where he teaches

courses covering Capital Markets/Digital Assets/Securities Regulation and Corporate Governance; State Capitalism, AML/Cybersecurity; Geopolitics/Geo-Economics, and U.S. Foreign Policy/International Relations, and Grand Strategy.

Mr. Jannace had previously worked at the American and New York Stock Exchanges, FINRA and several investment banking firms. He was also an account executive at Georgeson and D.F. King where he worked on proxy fights and tender offers. He has also served as a consultant for The World Bank and the Asian Corporate Governance Association. He has also lectured at the U.S. Army War College.

Mr. Jannace has also conducted overseas training programs for the: Russian Securities Commission/Stock Exchange; The Capital Markets Authorities in: Uganda, Burundi, Tanzania and Kenya; Saudi Arabian Capital Markets Authority; Securities and Exchange Board of India; Ukrainian Securities Commission/Stock Market; Romanian Securities Commission; Jordanian Securities Commission; Capital Markets Authority of Turkey; Albanian Financial Supervisory Authority; New York Institute of Finance- Beijing/China, the Taiwan Stock Exchange and for IOSCO in Spain.

He is a member of the faculty advisory group of Board Intelligence. He is also a CIArb Fellow, a member of the Association of Certified Anti Money Laundering Specialists, International Institute for Strategic Studies, New York International Arbitration Center, and Bretton Woods Committee. He is also a supporter of the National World War II Museum, American Battle Monuments Foundation, and National D-Day Memorial. Mr. Jannace received his JD from New York Law School, and his LL.M. in Corporate, Banking, and Finance Law from Fordham Law School.

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government. In addition, they do not reflect the official policy or position of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.
FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. www.fticonsulting.com.

23 Maytime Court
Jericho, NY 11753
+1 516 935 0923
www.GFMI.com

[1] Article 5 of the NATO Treaty: The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
North Atlantic Treaty Org., "The North Atlantic Treaty" (Apr. 4, 1949), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty.

[2] "Cyber attacks present a clear challenge to the security of the NATO Alliance and could be as harmful to modern societies as a conventional attack… Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain its freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defense: cyber defense will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success."
North Atlantic Treaty Org., "Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016," ¶ 70
(Jul. 9, 2016), https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique.

[3] For additional information, see Significant Cyber Incidents, a timeline that records significant cyber incidents since 2006, focusing on cyber attacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars.
"Significant Cyber Incidents," Center for Strategic & International Studies (March 2026), https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[4] "The principle of resilience is rooted in Article 3 of the North Atlantic Treaty: 'In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.'"

North Atlantic Treaty Org., "Resilience, Civil Preparedness and Article 3" (Nov. 13, 2024), https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3.

[5] There is widespread reluctance to invoke Article 5 of its founding treaty. When asked if their country should defend a fellow NATO ally against a potential attack from Russia, a median of 50% across 16 NATO member states say their country should not defend an ally, compared with 38% who say their country should defend an ally against a Russian attack.
Fagan, Moira & Poushter, Jacob, "NATO Seen Favorably Across Member States," Pew Research Center (February 9, 2020), https://www.pewresearch.org/global/2020/02/09/nato-seen-favorably-across-member-states/.

[6] North Atlantic Treaty Org., Resilience, Civil Preparedness and Article 3, supra note 4; In a 2018 report entitled, Europe's Responsibility to Prepare: Managing Climate Security Risks in a Changing World, The Center for Climate and Security, in partnership with the Clingendael Netherlands Institute of International Relations and in support of the Planetary Security Initiative, noted that the security threats of climate change should be more routinely integrated into EU institutions at a senior level and be elevated alongside other 'traditional' security issues like terrorism and nuclear threats. The report provided a detailed recommendations on what a response scaled to the threat of climate change across EU bodies could look like.
Fetzek, Shiloh & van Schaik, Louise, "Europe's Responsibility to Prepare: Managing Climate Security Risks in a Changing World," The Center for Climate and Security (June 2018), https://climateandsecurity.files.wordpress.com/2018/06/europes-responsibility-to-prepare_managing-climate-security-risks-in-a-changing-world_2018_6.pdf.

[7] North Atlantic Treaty Org., Resilience, Civil Preparedness, and Article 3, supra note 4.

[8] Id.

[9] Id.

[10] North Atlantic Treaty Org., "Funding NATO" (April 8, 2026), https://www.nato.int/en/what-we-do/introduction-to-nato/funding-nato.

[11] Fust, George J. LTC, "Competition Warfare: Strategic Terrain Is No Longer Geographic," Irregular Warfare Center (May 15, 2026), https://irregularwarfarecenter.org/publications/perspectives/competition-warfare-strategic-terrain-is-no-longer-geographic/.

[12] Congressional Research Service, "Cybersecurity: Selected Cyberattacks, 2012-2025" (May 18, 2026), https://www.congress.gov/crs_external_products/R/HTML/R46974.web.html#_Toc230095317. See also Condoleezza Rice, Jennifer Widom, Amy Zegart, Herbert S. Lin, & Martin Giles, "The

Stanford Emerging Technology Review 2026: A Report on Ten Key Technologies and Their Policy Implications," Stanford University (n.d.), https://setr.stanford.edu/sites/default/files/2026-02/SETR2026_web-260219.pdf.

[13] Id.

[14] Cybersecurity & Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure" (February 7, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[15] Cybersecurity & Infrastructure Security Agency, "Joint Statement by FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure" (November 13, 2024), https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications.
See also Ruiz, Ashley, "Machine Overmatch: What Salt Typhoon Reveals About China's Data-Centric Intelligence Strategy," War on the Rocks (May 20, 2026), https://warontherocks.com/machine-overmatch-what-salt-typhoon-reveals-about-chinas-data-centric-intelligence-strategy/.

[16] See FINRA Rule 4370 for additional information on mission critical systems.
"FINRA Rule 4370. Business Continuity Plans and Emergency Contract Information" (n.d.), https://www.finra.org/rules-guidance/key-topics/business-continuity-planning.

[17] Joyce, Rob, "China's Cyber Explosives are in Place. Where's our Response?" Cyber Defense Review (May 5, 2026), https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4477628/chinas-cyber-explosives-are-in-place-wheres-our-response/.

[18] United States Cyber Command, "Our History," U.S. Cyber Command (n.d.), https://www.cybercom.mil/About/History/.

[19] United States Cyber Command, "Academic Engagement," U.S. Cyber Command (n.d.), https://www.cybercom.mil/Partnerships-and-Outreach/Academic-Engagement/.

[20] U.S. Department of War, "Department of War Establishes CYBERCOM 2.0 – Revised Cyber Force Generation Model" (November 6, 2025), https://www.war.gov/News/Releases/Release/Article/4330204/department-of-war-establishes-cybercom-20-revised-cyber-force-generation-model/.

[21] U.S Department of the Treasury, "U.S. Department of the Treasury Releases Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Sector" (March 27, 2024), https://home.treasury.gov/news/press-releases/jy2212.

[22] Id.

[23] Project Glasswing brings together Amazon Web Services, Anthropic, Apple, Broadcom, Cisco, CrowdStrike, Google, JPMorganChase, the Linux Foundation, Microsoft, NVIDIA, and Palo Alto Networks in an effort to secure the world's most critical software. It was formed due to the capabilities Anthropic has observed in a new frontier model trained by it that it believes could reshape cybersecurity. Claude Mythos Preview is a general-purpose, unreleased frontier model that reveals that AI models have reached a level of coding capability where they can surpass all but the most skilled humans at finding and exploiting software vulnerabilities. Given the rate of AI development, its capabilities will proliferate, potentially beyond actors who are committed to deploying them safely. The potential negative economic and national security fallout could be severe. Anthropic' s Project Glasswing is an attempt to put these capabilities to work for defensive purposes.
"Project Glasswing," Anthropic (April 7, 2026), https://www.anthropic.com/glasswing.

[24] Azhar, Saeed, "Bessent, Powell warned bank CEOs about Anthropic model risks, sources say," Reuters (April 10, 2026), https://www.reuters.com/business/finance/bessent-powell-warn-bank-ceos-about-anthropic-model-risks-bloomberg-news-reports-2026-04-10/.

[25] Sims, Tom, et al, "Banking industry scrambles for Anthropic's Mythos as global regulators review risks," Reuters (April 20, 2026), https://www.reuters.com/business/finance/banks-close-contact-with-european-regulator-anthropics-mythos-banker-says-2026-04-20/.

[26] "Expanding Project Glasswing," Anthropic (June 2, 2026), https://www.anthropic.com/news/expanding-project-glasswing.

[27] FINRA Rule 4370 gives a firm flexibility in designing a BCP. It may be tailored to the size and needs of the firm, but at a minimum it must include the following elements: Data backup and recovery (hard copy and electronic); All mission critical systems; Financial and operational assessments; Alternate communications between customers and the firm, and between the firm and employees; Alternate physical location of employees; Critical business constituent, bank, and counterparty impact; Regulatory reporting; Communications with regulators; and How the firm will assure customers' prompt access to their funds and securities in the event that the firm determines that it is unable to continue its business. A firm must address the elements to the extent applicable and necessary. If any of the elements is not applicable, the firm's BCP must document the rationale for not including the element in its plan. If a firm relies on another entity for any one of the elements or any mission critical system, the firm's BCP must address this relationship. FINRA provides optional tools to assist firms in in fulfilling their need to create and maintain business continuity plans (BCPs) and emergency contact person lists under FINRA Rule 4370.
"FINRA Rule 4370. Business Continuity Plans and Emergency Contact Information" (n.d.), https://www.finra.org/rules-guidance/key-topics/business-continuity-planning.

[28] FINRA, "Business Continuity Plan Template for Small Introducing Firms" (2026), https://www.finra.org/sites/default/files/2026-04/BCP_Template.pdf.

[29] Id.

[30] The 2025 SIFMA Industry Test and Reg SCI testing included approximately one hundred securities firms and over eighty market organizations. During the industry test approximately 1,100 communications connections were established between securities firms and banks and the exchanges, markets, and utilities. Test transactions on these connections were successful approximately 98% of the time. Results were comparable to prior tests and underscore the ability of the industry to operate through adverse conditions. Industry testing to meet the requirements of Regulation Systems Compliance and Integrity (Reg SCI) also took place in parallel with the SIFMA industry test. Securities Industry and Financial Markets Association, "Industry-Wide Business Continuity Test" (October 25, 2025), https://www.sifma.org/resources/readiness-exercises/industry-wide-business-continuity-test.

[31] Id.

[32] Securities and Exchange Commission, "Regulation S-P" (n.d.), https://www.sec.gov/spotlight/regulation-s-p.htm.

[33] Covered institutions include broker-dealers (including funding portals), investment companies, registered investment advisers, and transfer agents.
FINRA, "Cybersecurity Advisory – SEC Amends Regulation S-P Enhancing Protection of Customer (Exchange Act Release No. 35193)" (n.d.), https://www.finra.org/rules-guidance/guidance/cybersecurity-advisory-sec-amends-regulation-s-p.

[34] Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (July 26, 2023), https://www.sec.gov/rules-regulations/2023/07/s7-09-22.

[35] "Vendor Breaches Create a New SEC Compliance Test," PYMNTS (May 7, 2026), https://www.pymnts.com/cybersecurity/2026/security-exchange-commission-new-30-day-reporting-rule-puts-vendors-cybersecurity-crosshairs/.

[36] Policy Statement: Business Continuity Planning for Trading Markets Exchange Act Release No. 34-48545, 68 Fed. Reg. 56,656 (October 1, 2003), https://www.sec.gov/rules-regulations/policy-statements/34-48545.

[37] After the issuance of this guidance, the SEC established the Consolidated Audit Trail (CAT) to enable regulators to track all order and trading activity across U.S. markets for listed equities and options. Operated by 25 Self-Regulatory Organizations (SROs), including equity and options exchanges, and under SEC supervision, the CAT is designed to strengthen market oversight and transparency by providing a comprehensive view of trade data. Securities Industry and Financial Markets Association, "Consolidated Audit Trail (CAT)" (n.d., https://www.sifma.org/issues/regulatory-compliance/consolidated-audit-trail.

The CAT tracks orders throughout their life cycle and identifies the broker-dealers handling them, thus allowing regulators to efficiently track activity in Eligible Securities throughout the U.S. markets. Id.

[38] Exchange Act Release No. 34-48545, 68 Fed Reg, at 56,658.
The Securities Industry Financial Markest Association led an annual industry-wide business continuity test, in which Self-Regulatory Organizations (SROs) such as NASDAQ and NYSE participated. Securities Industry and Financial Markets Association., Industry-Wide Business Continuity Test, supra note 30.

[39] "When Milliseconds Define Billions and Human Error Meets Algorithmic Speed," Verified Investing (n.d.), https://verifiedinvesting.com/blogs/education/flash-crashes-and-fat-fingers-when-technology-turns-against-the-markets?srsltid=AfmBOorPVQqNfqmzH3oKOmgTFQHqQwI1bhtMaS2q6Uk4xFXvCo73IBEQ. See also Scaggs, Alexandra, "Floor Traders Praise NYSE Officials' Handling of Trading Glitch," Wall Street Journal (August 1, 2012), https://www.wsj.com/articles/BL-MB-43376.

[40] Each SCI Entity is required to implement reasonably designed written policies and procedures to ensure that its "SCI Systems" and Indirect SCI Systems are able to maintain the SCI Entity's operational capabilities and promote fair and orderly markets. "SCI Systems" are an SCI Entity's systems that support trading, clearance and settlement, order routing, market data (both consolidated and proprietary), market regulation, and market surveillance. Indirect SCI Systems are those systems of the SCI Entity or those of a third party operated by or on behalf of an SCI Entity, that if breached, would be reasonably likely to pose a security threat to SCI Systems. The SCI Entity's policies and procedures must include, among other things, business continuity and disaster recovery plans that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of certain "critical SCI systems" following a wide-scale disruption. An SCI Entity's policies and procedures would be deemed reasonably designed if they are consistent with widely recognized industry standards, examples of which have been published by the SEC staff.
Nazareth, Annette L., "SEC Adopts Regulation SCI to Strengthen Securities Market Infrastructure," Harvard Law School Forum on Corporate Governance (January 7, 2015), https://corpgov.law.harvard.edu/2015/01/07/sec-adopts-regulation-sci-to-strengthen-securities-market-infrastructure/.

[41] Regulation Systems Compliance and Integrity, Exchange Act Release No. 34-73639, 79 Fed. Reg. 72,252 (December 5, 2014), https://www.sec.gov/rules-regulations/2015/12/regulation-systems-compliance-integrity.

[42] Lyudvig, Anna, "Trading Firms Rethink Risk Controls as Settlement Timelines Compress," Traders Magazine (May 15, 2026), https://www.tradersmagazine.com/featured_articles/trading-firms-rethink-risk-controls-as-settlement-timelines-compress/.

[43] Id.

[44] "FINRA Rule 4380. Mandatory Participation in FINRA BC/DR Testing Under Regulation SCI" (November 3, 2015), https://www.finra.org/rules-guidance/rulebooks/finra-rules/4380.

[45] Carrying agreements between an introducing firm and its carrying (clearing) firm must, at a minimum, specify the responsibilities of each party with respect to: Opening and approving accounts; Acceptance of orders; Transmission of orders for execution; Execution of orders; Extension of credit; Receipt and delivery of funds and securities; Preparation and transmission of confirmations; Maintenance of books and records; and Monitoring of accounts "Carrying Agreements," Master Compliance (December 31, 2021), https://mastercompliance.com/blog/carrying-agreements/.

[46] "FINRA Rule 4311. Carrying Agreements" (n.d.), https://www.finra.org/rules-guidance/rulebooks/finra-rules/4311.

[47] In 2005, FINRA issued Notice to Members 05-48 (Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers), which identified common activities or functions that member firms frequently outsourced to third-party providers, including: accounting and finance services, such as payroll and expense account reporting; legal and compliance services, such as outside counsel, anti-money laundering monitoring and cyber insurance providers; information technology (IT) and cybersecurity, such as software support, IT help desk support centers, cloud service providers, managed detection and response providers; business operations functions, such as statement production and disaster recovery services; and administrative functions, such as human resources, employee benefits services or internal audits.
"Notice to Members 05-48: Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers," FINRA (July 22, 2005), https://www.finra.org/rules-guidance/notices/05-48.
Subsequently, FINRA member firms have continued to expand the scope and depth of their use of technology. As noted in *Regulatory Notice 21-29* (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors), member firms increasingly leveraged third-party providers to perform risk management functions and assist in supervising sales and trading activity and customer communications.
FINRA Cyber and Analytics Unit, "Cybersecurity Advisory – Increasing Cybersecurity Risks at Third-Party Providers," FINRA (n.d.), https://www.finra.org/rules-guidance/guidance/cybersecurity-advisory-third-party-provider-risks.
"Regulatory Notice 21-29: FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors," FINRA (August 13, 2021), https://www.finra.org/rules-guidance/notices/21-29. In addition, in 2023, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency jointly issued Interagency Guidance on Third-Party Relationships: Risk Management, which provides guidance to help banking organizations manage risks associated with third-party provider relationships.

Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37,920 (June 9, 2023), https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf.

[48] FINRA Cyber and Analytics Unit, "Cybersecurity Advisory – Increasing Cybersecurity Risks at Third-Party Providers," FINRA (n.d.), https://www.finra.org/rules-guidance/guidance/cybersecurity-advisory-third-party-provider-risks.
In 2023, the Cybersecurity and Infrastructure Agency (CISA) published Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks, which provides guidance for SMBs that serve as third-party providers of IT and communications services. ICT Supply Chain Risk Management (SCRM) Task Force, "Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks," Cybersecurity & Infrastructure Security Agency (CISA), (January 26, 2023), https://www.cisa.gov/resources-tools/resources/securing-smb-supply-chains-resource-handbook.

[49] FINRA Cyber and Analytics Unit, supra note 48.

[50] Id.

[51] "Cybersecurity," FINRA (2026), https://www.finra.org/rules-guidance/key-topics/cybersecurity.

[52] "Cyber Workshops & Tabletop Exercises – Prepare for Potential Cybersecurity Events," FINRA (n.d.), https://www.finra.org/sites/default/files/2025-07/Cyber_Workshops_and_Tabletop_Exercises.pdf.

[53] "Cyber & Operational Resilience (CORE)," FINRA (2026), https://www.finra.org/sites/default/files/2025-07/FINRA_CORE.pdf.

[54] "FINRA Launches Financial Intelligence Fusion Center to Combat Cybersecurity and Fraud Threats," FINRA (March 31, 2026), https://www.finra.org/media-center/newsreleases/2026/finra-launches-financial-intelligence-fusion-center-combat.

[55] Securities Industry and Financial Markets Association, Industry-Wide Business Continuity Test, supra note 30.

[56] During an industry-wide incident, SIFMA notes that it convenes market participants, coordinates with the U.S. Department of the Treasury, Department of Homeland Security, New York City Office of Emergency Management, and other agencies, and issues market close recommendations. Its market response committees for the fixed income and equity markets ensure decisions are consistent with securities regulators' expectations for resiliency and continuity.
Securities Industry and Financial Markets Association, "Operational Resilience and Cybersecurity"

(n.d.), https://www.sifma.org/issues/financial-risk-management/operational-resilience-cybersecurity.

[57] Id.

[58] "Cybersecurity Framework," National Institute of Standards and Technology (n.d.), https://www.nist.gov/cyberframework.

[59] "The Profile," Cyber Risk Institute (n.d.), https://cyberriskinstitute.org/the-profile/.

[60] Securities Industry and Financial Markets Association, Operational Resilience and Cybersecurity, supra note 56.

[61] Since 9/11, Quantum Dawn exercises have brought together industry leaders, government agencies, and other key stakeholders to simulate large-scale cyber incidents and test the operational resilience of the U.S. financial system. Id.

[62] See supra note 57.

[63] SIFMA Operations & Technology Committee, "Cybersecurity Exercise: Quantum Dawn VIII," SIFMA (March 30, 2026), https://www.sifma.org/resources/readiness-exercises/cybersecurity-exercise-quantum-dawn-viii.
SIFMA Operations & Technology Committee, "Quantum Dawn Cybersecurity Exercises," SIFMA (November 4, 2025), https://www.sifma.org/resources/readiness-exercises/quantum-dawn-cybersecurity-exercises.

[64] The exercise included nearly 1,000 participants from more than one hundred public and private sector institutions around the world, including financial firms, regulatory bodies, central banks, law enforcement, government agencies, trade associations, and information-sharing organizations.
SIFMA Operations & Technology Committee, "SIFMA's Quantum Dawn VIII Exercise Tests Readiness for Polycrisis Incidents," SIFMA (March 30, 2026), https://www.sifma.org/news/press-releases/sifmas-quantum-dawn-viii-exercise-tests-readiness-for-polycrisis-incidents.

[65] Id.

[66] "Protecting Financial Stability," Carnegie Endowment for International Peace (n.d.), https://carnegieendowment.org/projects/protecting-financial-stability/fincyber-strategy-project-working-group-on-cybersecurity-workforce.

[67] Maurer, Tim and Nelson, Arthur, "International Strategy to Better Protect the Financial System Against Cyber Threats," Carnegie Endowment for International Peace (November 18, 2020),

https://carnegieendowment.org/research/2020/11/international-strategy-to-better-protect-the-financial-system-against-cyber-threats.

[68] "Protecting Financial Stability: Protecting the global financial system against cyber threats," Carnegie Endowment for International Peace (n.d.), https://carnegieendowment.org/projects/protecting-financial-stability/about-the-fincyber-strategy-project.

[69] "Fostering Innovation," Bank for International Settlements (2023), https://www.bis.org/about/areport/areport2023/5_fost_innov.htm.

[70] The G7 Cyber Expert Group (CEG) meets regularly to identify the leading cybersecurity risks in the financial sector and to propose actions to be taken in this area. U.S. Treasury and the Bank of England chair the CEG. While not an SSB, the CEG nonetheless helps drive the development of international cybersecurity policies across the G7 (and beyond) through its publication of "fundamental elements." Notably, it published the "G7 Fundamental Elements of Cybersecurity for the Financial Sector" in October 2016 and the "G7 Fundamental Elements for Effective Assessment of Cybersecurity" in October 2017.
"G7 Cyber Expert Group," U.S. Department of the Treasury (n.d.), https://home.treasury.gov/policy-issues/international/g-7-and-g-20/g7-cyber-expert-group.

[71] This document provides actionable guidelines for public and private sector stakeholders on what is reasonable to expect in a Software Bill of Materials (SBOM) for AI, and to improve transparency and cybersecurity along the AI supply chain. It builds on the vision of SBOM for AI published by the G7 Cybersecurity Working Group in June 2025 and provides useful practical recommendations on which minimum elements SBOMs for AI should include. "Software Bill of Materials for AI-Minimum Elements," Cybersecurity & Infrastructure Security Agency (May 12, 2026), https://www.cisa.gov/resources-tools/resources/software-bill-materials-ai-minimum-elements.

[72] See supra note 57.

[73] Id.

[74] The European Supervisory Authorities (ESAs) consists of the European and Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA).
"European system of financial supervision," European Commission (December 4, 2025), https://finance.ec.europa.eu/regulation-and-supervision/european-system-financial-supervision_en.

[75] The European Union introduced the Digital Operational Resilience Act (DORA) to strengthen the digital resilience of financial entities. It ensures that banks, insurance companies, investment firms,

and other financial entities can withstand, respond to, and recover from Information and Communication Technology disruptions, such as cyber attacks or system failures.
Digital Operational Resilience Act (DORA), European Insurance and Occupational Pensions Authority (n.d.), https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

[76] Tote, Hansa, "ESAs publish first DORA report on ICT incidents," Securities Finance Times (June 3, 2026), https://www.securitiesfinancetimes.com/securitieslendingnews/technologyarticle.php?article_id=228716.

[77] Id.

[78] Id.

[79] See generally on the evolving geopolitical tensions and regulatory expectations that are transforming compliance obligations for the financial services sector, redefining their role from transaction facilitators and processors to frontline disruptors and defenders of national security interests.
Angotti, Alma, et al, "Financial Institutions at the Crossroads of National Security and Compliance," FTI Consulting (March 2, 2026), https://www.fticonsulting.com/insights/articles/financial-institutions-crossroads-national-security-compliance.

[80] "2025 Annual Report," Financial Stability Oversight Council (2025), https://home.treasury.gov/system/files/261/FSOC2025AnnualReport.pdf.

[81] The White House, "President Trump's Cyber Strategy for America" (March 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.

[82] The White House, "Promoting Advanced Artificial Intelligence Innovation and Security" (June 2, 2026), https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/.

[83] The Financial Services Sector Coordinating Council (FSSCC) was established in 2002. It is an industry-led, non-profit organization that coordinates critical infrastructure and homeland security activities within the financial services industry. Its members consist of financial trade associations, financial utilities, and the most critical financial firms.
"Welcome page," Financial Services Sector Coordinating Council (2026), https://fsscc.org/. See also U.S. Department of the Treasury, "Treasury Announces Public-Private Initiative to Strengthen Cybersecurity and Risk Management for AI" (February 18. 2026), https://home.treasury.gov/news/press-releases/sb0395 and The White House, "Winning the

Race America's AI Action Plan" (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

[84] "Financial Services Sector Risk Management Plan," U.S. Department of the Treasury (January 2025), https://home.treasury.gov/system/files/216/Financial-Services-Sector-Risk-Management-Plan.pdf.

[85] Chartered under the President's Working Group on Financial Markets, the Financial and Banking Information Infrastructure Committee (FBIIC) is charged with improving coordination and communication among financial regulators, promoting public-private partnerships within the financial sector, and enhancing the resiliency of the financial sector overall.
"Financial and Banking Information Infrastructure Committee," FBIIC (n.d.), https://www.fbiic.gov/.

[86] Id.

[87] See note 84.

[88] Id.

[89] In a recent report, Google explained that future quantum computers may break the elliptic curve cryptography that protects cryptocurrency and other systems with fewer qubits and gates than previously projected. Google noted that it was seeking to raise awareness on this issue and to provide the cryptocurrency community with recommendations to improve security and stability before this is possible, including transitioning blockchains to post-quantum cryptography (PQC), which is resistant to quantum attacks. Babbush, Ryan & Neven, Hartmut, "Safeguarding Cryptocurrency by Disclosing Quantum Vulnerabilities Responsibly," Google Research (March 31, 2026), https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/.

[90] While not directly related to cybersecurity, federal guidance in connection with the recently passed Genius Act provides insights into subtle changes to the focus of regulation. The Treasury's FinCEN and OFAC proposed rulemaking to implement the GENIUS Act's anti-money laundering and sanctions compliance program requirements.
Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements,91 Fed. Reg. 18,582 (April 10, 2026), https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism.
Notably, proposed rulemaking provides that payment stablecoin issuers (PPSIs) ***must have the technical capability to block, freeze, and reject impermissible transactions on both primary and secondary markets, and they must prevent sanctioned persons from interacting with their smart contracts including in P2P transactions between self-hosted wallets.***
"Treasury Proposes Rule to Implement the GENIUS Act's Requirements to Counter Illicit Finance,"

U.S. Department of the Treasury (April 8, 2026), https://home.treasury.gov/news/press-releases/sb0435.

[91] Ray, Timothy, "Rethinking Corporate Risk and Alignment in an Era of Economic Statecraft," War on the Rocks (April 30, 2026), https://warontherocks.com/rethinking-corporate-risk-and-alignment-in-an-era-of-economic-statecraft/.

[92] The White House, "National Cybersecurity Strategy" (March 2023), https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
A coordinated national system that integrates government, private industry, academia, and national laboratories into a unified cybersecurity ecosystem is needed to address cyber risks that transcend institutional boundaries, targeting critical infrastructure, and economic systems, requires synchronized action across all sectors of society. Moreover, resilience in cyberspace depends not only on technological advancement but on collective responsibility and sustained national commitment to shared defense.
See Myers, Ross A., "Embracing a Whole-of-Nation Approach to the 2026 National Cybersecurity Strategy Inspired by the Manhattan Project," Cyber Defense Review (May 4, 2026), https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4476826/embracing-a-whole-of-nation-approach-to-the-2026-national-cybersecurity-strateg/.

[93] The White House, "National Cybersecurity Strategy" (March 2023), https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
Joyce, Rob, "China's Cyber Explosives are in Place. Where's our Response?" Cyber Defense Review, (May 5, 2026), https://cyberdefensereview.army.mil/CDR-Content/Articles/.
See also O'Brien, Mary, "Wrong Players, Wrong Game: Rethinking Who Belongs in Cyber," Cyber Defense Review (May 4, 2026), https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4476619/wrong-players-wrong-game-rethinking-who-belongs-in-cyber/.

[94] See Arnold, Aaron, "Algorithms of Evasion: The Rise of AI-Enabled Proliferation Financing," The Royal United Services Institute for Defence and Security Studies (May 26, 2026), https://www.rusi.org/explore-our-research/publications/research-papers/algorithms-evasion-rise-ai-enabled-proliferation-financing, in which he advocates for the implementation of 'circuit breakers' for API-initiated transactions, designed to automatically freeze high-speed, cross-border fund transfers that show signs of being directed by autonomous AI agents for human review.