Acting Comptroller of the Currency Michael J. Hsu

Remarks before the Joint Meeting of

the Financial and Banking Information Infrastructure Committee and

the Financial Services Sector Coordinating Council

August 2, 2022

Thank you for the kind introduction and for inviting me to speak today. I'm very glad to be speaking at this forum given the important roles that the FBIIC and FSSCC play in enhancing cybersecurity and resilience, and the significant progress in collective action for which those bodies have been responsible.

My remarks today are framed by three intersecting risks that require our individual and collective vigilance: the risk of evolving cybersecurity threats, the risk to critical operations, and the risk of complacency.

To date, the industry overall has done a good job of building cyber defenses and working with law enforcement and the regulatory community to guard against attacks. Those efforts and the cooperative engagement underlying them deserve recognition.

My sense, however, is that success can breed a false sense of security. We cannot be complacent. In a world of constantly evolving threats, vigilance must be maintained, especially when things are quiet. And with increasingly complex dependencies in the provision of financial services, heightened focus on the resilience and recovery capabilities of critical operations is imperative.

Evolving Threats and Cyber Risks

Information technology systems are relied on for the delivery of nearly all financial services in the federal banking system. Advances in technology have driven innovation through new products, services, and delivery channels developed to meet evolving customer needs, preferences, and service expectations. The OCC recognizes the critical role responsible innovation serves in allowing financial institutions of all sizes to have access to new technologies that increase productivity and provide a wider range of products and services to customers. At the same time, however, we recognize these same advances have also contributed to an increasingly complex and interconnected operating environment that has resulted in increased cyber risk. The threats for many financial institutions continue to expand at a rapid pace as the interconnectedness of multiple specialized service providers and fintechs increases, digitalization of critical infrastructure components proliferates, and reliance on cloud services grows rapidly. These developments support new and innovative services and facilitate the emerging hybrid workforce of remote and on-site employees accessing critical services through a web of interconnected devices.

In addition, we have observed increases in the frequency and severity of cyber attacks against financial institutions and their service providers in recent years. Disruptive and destructive cyber attacks, such as ransomware, targeted at the financial sector have elevated risks beyond the mere threat of financial loss. Disruption to financial services can significantly impact banks' abilities to deliver critical services to their customers and has the potential to affect the broader economy. Many of the largest financial institutions, which are represented in this room, not only support their own customers, but also support critical activities including wholesale payments, trade settlement, and custody. Financial institutions need to assess both the potential

impact cyber incidents may have on their own institution and the impact a cyber disruption may have on the broader financial system. Even relatively unsophisticated attacks can cause significant damage and disruption under the right conditions.

While most cyber incidents we have observed in recent years have been primarily financially motivated in nature, Russia's invasion of Ukraine has highlighted how geopolitical tensions can further increase cyber risks to the financial sector. In the lead-up to, and escalation of, hostilities, firms in the region were targeted with destructive cyber attacks that had the potential to delete information permanently and disable operations. These were not financially motivated attacks that could be mitigated by a ransom payment or insurance coverage. Although the most acute of these attacks have been isolated so far to the region, it would be wise to heed the warning that these threats represent and act accordingly to improve our collective defenses.

Vigilance and Investment in Cyber Defenses

The increasing interconnectedness and complexity of today's operating environment and the continued cyber threats pose a growing safety and soundness risk to banks and the broader financial sector if not properly managed. It is essential that financial institutions continue both to invest in building a secure and resilient infrastructure and to collaborate through public/private partnerships, such as the coordinated efforts of the FBIIC and FSSCC to strengthen the defense of the financial sector.

We recognize and applaud the significant resource investments financial institutions have made in technology and services to improve their ability to identify and recover from various types of potential disruptions. And while many experts view the financial industry as one of the more mature sectors for cybersecurity preparedness, we remain susceptible to a wide range of

cyber and operational risks. These risks underscore the importance for financial institutions of all sizes not only to maintain increased cybersecurity vigilance, but also to ensure that they maintain adequate operational resilience to recover and continue critical operations in the event of a cyber disruption. Cybersecurity strategies should be tailored according to the size and complexity of financial institutions, their risk appetite, and the role they play in the sector's critical infrastructure, including critical third parties that support operations.

Our observations from a regulatory perspective indicate that effective management of basic cybersecurity controls can significantly contribute to enhancing the resilience of systems and operations against cyber threats. We have observed that the majority of cybersecurity breaches have been caused or exacerbated by failure to have effective controls in the following three areas:

- strong authentication;
- effective systems configuration and patch management; and
- cyber response and resilience capabilities.

The first line of defense against malicious cyber actors is the implementation of strong preventative controls to protect against unauthorized access. Last August, through the FFIEC, we updated our authentication guidance to highlight how the base layer security approach of multifactor authentication, or controls of equivalent strength, can significantly strengthen controls to mitigate unauthorized access to systems and data. All financial institutions should implement effective multifactor authentication controls for access to all nonpublic systems, as even basic network systems can be entry points for malicious activity.

I cannot overstate the importance of investing in processes to ensure the effective design and configuration of infrastructure and patch management applications. After credential threat,

the next most common contributing factor to cyber breaches at financial institutions has been the result of misconfigured or unpatched systems. Malicious actors are very familiar with the security settings of commonly used software products throughout the industry and often seek misconfigured or unpatched systems applications to exploit.

While these fundamental blocking or preventive controls—threat monitoring, vulnerability patching, identity and access management, cyber incident response planning—are important to reduce risk, financial institutions should also be prepared for potential cyber disruptions and maintain sufficient resilience through effective incident response processes and rapid recovery in the event that preventative controls are not sufficient to safeguard against a cyber event. A key component of these capabilities is to establish controls to safeguard the integrity and availability of critical data against the impact of destructive malware. Recovery from such incidents may include procedures for the restoration of immutable, off-line data. Industry groups are leading various efforts, such as Sheltered Harbor and the Global Resilience Federation, to ensure that there are standardized, developed practices and frameworks to support recovery and restoration of critical data. We have observed that the integrity of backup systems for critical data has greatly influenced banks' ability to respond to ransomware and other malware events.

Cyber Preparedness and Resilience at the OCC

Cyber threats to the financial sector are not limited solely to financial institutions, and the OCC recognizes that the scope of these threats is much broader. The OCC recently released our spring 2022 *Semiannual Risk Perspective*,[1] highlighting the current cyber threat environment and

[1] See https://www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/semiannual-risk-perspective-spring-2022.html

the importance of not only financial institutions maintaining effective cybersecurity controls, but also the important role third-party service providers and the overall supply chain play in the resilience of the sector. Similarly, the OCC's bank supervision operating plan highlights cybersecurity as a key area of focus for the agency's supervisory strategy across banks and critical service providers, as we work closely with our interagency counterparts. The OCC also recognizes that we are also exposed to cyber threats and have taken steps to ensure that our agency has effective cybersecurity controls and resilience that meet both federal and industry standards. We document the agency's supervisory and internal cybersecurity efforts through our annual *Cybersecurity and Financial System Resilience Report* to Congress, which is available on OCC.gov.[2]

Collective Defenses and Partnerships with Industry and Law Enforcement

In light of the environment I have described, collaboration and harmonization among public and private-sector stakeholders are critical to safeguarding and maintaining confidence in the financial sector. Developing true collective defense capabilities will make the financial sector stronger and more resilient and will also require new modes of interaction and coordination among stakeholders. Rapidly evolving cybersecurity risks also reinforce the need for institutions and their service providers to partner on the implementation of appropriate methods for identifying, monitoring, sharing, and responding to threat and vulnerability information.

We at the OCC are strong believers in the value of and need for true collaboration to address cyber risks. U.S. National Cyber Director Chris Inglis and Assistant Director Harry Krejsa have called for a "new contract" where "both the public and private sectors must commit

[2] See https://www.occ.gov/publications-and-resources/publications/banker-education/files/2022-cybersecurity-report.html

to moving toward true collaboration—contributing resources, attention, expertise, and people toward institutions designed to prevent, counter, and recover from cyber-incidents."[3] With the increasing cyber threat environment, it is imperative for government and financial firms to share threat information for the benefit of the entire sector. Director Inglis and Assistant Director Krejsa laid out a vision for the allocation of risks and responsibilities assumed by public and private actors. What especially resonates with me was their articulation of the need to build a shared consciousness across government and the private sector.

To do that, information needs to flow quickly and easily to where it is most useful so those at risk can effectively monitor and safeguard against cyber threats and government agencies can fulfil their respective missions of safety and soundness, financial stability, consumer protection, and protection of the critical infrastructure of the United States.

Of course, we need to be smart about how we collaborate. Timeliness is important. We need to ensure that the collection of information is efficient, targeted, proceeds along streamlined delivery channels, and avoids unnecessary burden.

To that end, we continue to encourage banks to participate actively in information-sharing forums as an important element of risk management processes. An example of this type of collaboration is the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which has been vital in providing an information-sharing forum of physical and cybersecurity threat and vulnerability information. This forum has also given community banks and smaller financial institutions with limited resources access to current threat information and best practices to guard against known and emerging cyber threats.

[3] See "The Cyber Social Contract," *Foreign Affairs,* February 21, 2022, https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract

To facilitate this community sharing further, there have been a number of government efforts addressing the reporting of cyber incidents. For example, the OCC, along with our federal banking agency partners, implemented the Computer-Security Incident Notification Rule to ensure timely notification to the primary regulator when a cyber attack impacts operations or the ability to provide services to customers.

These requirements not only provide government agencies with early awareness of emerging threats to the financial sector but also allow for better assessment of potential impact and support responses across the financial sector and institutions of all sizes. The information can also support law enforcement efforts to target cyber threat actors and enable the Cybersecurity and Infrastructure Security Agency, or CISA, to share better cyber threat intelligence more effectively.

I am committed to working with CISA, our financial sector counterparts, and other sectors to ensure that we have strong partnerships across the government. Such strong partnerships create efficient processes that benefit all stakeholders, manage burden, and enhance the sector's ability to respond to cyber threats.

I ask both the private and public sector representatives gathered here today to join me in this commitment to work collaboratively on streamlining the incident report and threat information-sharing process. By doing so, we ensure that critical information is shared with required stakeholders on a timely basis, while working to eliminate duplicative or unnecessary burdens. In this manner, we can work to approach ongoing threats to our sector as a community to strengthen the collective defense of the financial sector and the nation.

Thank you.