World Council

December 22, 2022

<u>Delivered Via Email: FSB@fsb.org</u>

Dietrich Domanski
Secretary General/Secretariat
Financial Stability Board (FSB)
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting

Dear Secretary Domanski:

World Council of Credit Unions (World Council) appreciates the opportunity to comment on Financial Stability Board's (FSB) **Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting**.[1] Credit unions are cooperative depository institutions and World Council is the leading trade association and development organization for the international credit union movement. Worldwide, there are over 87,000 credit unions in 118 countries with USD 3.4 trillion in total assets serving 393 million physical person members.[2]

World Council applauds the efforts of the FSB's efforts to achieve greater convergence in cyber incident reporting (CIR). World Council concurs with the findings that cyber incidents are growing in frequency and sophistication and the risk of contagion across borders and sectors due to the growing interconnectedness of the financial system is likewise increasing. The FSB's focus on increasing the sharing of timely and accurate information is well placed to create a system that is effective for incident response, recovery, and promoting financial stability. We also concur with many of the impediments identified in achieving efficiencies in incident reporting.

While these overall goals and objectives are laudable, we are concerned that the implementation of many of the proposals designed to achieve these goals often become unworkable or prohibitively costly for smaller, less-complex financial institutions such as credit unions and other financial cooperatives. Credit unions and other financial cooperatives often report to us that the costs and regulatory burdens associated with regulatory requirements are barriers to serving their members. Credit unions often have limited financial and staff resources because of their relatively small size and are typically run by volunteer boards and volunteer

[1] *See* Financial Stability Board, Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting *available at:* https://www.fsb.org/wp-content/uploads/P171022.pdf.
[2] World Council of Credit Unions, *2021 Statistical Report* (2022), *available at*: https://www.woccu.org/our_network/statreport.

employees. In the European Union for example the average size of a credit union is EUR 11 million in total assets. This exacerbates the impact of any new reporting requirements.

New regulatory requirements always fall disproportionately to credit unions compared to large banks that have much greater economies of scale. Credit unions often have to rely on outside firms and vendors to provide solutions for their compliance and technology needs. Those systems often require a substantial amount of resources and labor and often come at a steep price. This is often true with new technology or digitalization efforts. Finally, with respect to cyber incidents it should be noted that credit unions worldwide rarely operate on a cross-border basis, thus reducing the risk of their institutions becoming a contagion or having a “spill-over” across borders or sectors.

To this end, the inclusion of proportionality in any scheme is imperative and needs to include a minimization of the number disclosures, reduction in the number of agencies to whom a credit union needs to report, and finally, ample timelines for compliance are imperative (along with financial support to implement the reforms). We urge considerations and inclusion of direction to national-level regulators to implement proportionality when imposing any new scheme to the extent possible. We note that the recently adopted Digital Operational Resilience Act (DORA) in the European Union, which creates a regulatory framework on digital operational resilience to ensure that firms can withstand, respond to and recover from all types of ICT-related disruptions and threats provides discretion to national-level regulators for those institutions exempt under CRD IV (CRD IV exempt under Article 2(5) of Directive 2013/36/EU). This approach was taken due to the smaller size, less complex nature of these financial institutions coupled with their lack of cross-border operations.

Credit unions will still be required to have policies and procedures in place to withstand ICT-related incidents, but those can be properly tailored to their size, risk, and complexity. Further, incident reporting can be done through an existing prudential regulator or other existing authority without imposing new systems or forms that need to be adopted. This can greatly reduce the regulatory burden of credit unions, while still integrating them into an effective broader system looking to achieve convergence.

Turning to some of the specific proposals, we support the FSB’s review and updates to the Cyber Lexicon. In particular, we believe the definition of a “cyber incident” should be limited to malicious incidents (or those with clear intent) with a corresponding high threshold for reporting. This will focus efforts on those incidents that pose the highest threat to the sector. Those incidents that are clearly contained or are non-material should not be treated in the same manner. This focus will allow the sector to allocate resources on those threats that actually pose danger to the sector, while limiting unnecessary regulatory burden on smaller financial institutions.

On information sharing, WOCCU observes that privacy frameworks vary widely from jurisdiction to jurisdiction and thus we urge inclusion of a recommendation to provide safe-harbors for reporting incidents than can transcend governmental borders. Many jurisdictions have become quite litigious thus acting as a barrier or hesitation to reporting. Reporting should be able to be accomplished freely without concern for unintended reprisals. Finally, with respect to information sharing, we urge the consultation to also focus on information from authorities to financial institutions where intelligence on incidents can be provided to a financial institutions in a timely and accurate manner. This is critical to enable a financial institution to take appropriate steps to mitigate any incident.

With respect to the (Section 5) Format for Incident Reporting Exchange (FIRE) reporting, we concur with FSB's observations that there will be implementation costs involved in changing existing regulatory policies and rules to support implementation as well as an unappealing "cost of entry" where the overall one-ff costs involved with implementation and migration may be less palatable than the current recurring overhead of operational challenges. We believe, this may also understate the costs for smaller-less complex financial institutions.

With regard to FIRE, if implemented, we urge flexibility in the format and flexibility for the authorities in implementation so that items can be tailored at the national-level. We urge particular direction to keep the forms simple, easily understandable, and focused only on providing the information that is necessary and actionable. We further urge strong direction for national authorities to allow reporting through an existing prudential or supervisory authority so as to not create additional unnecessary bureaucracy. All of these items will help with proportionality for credit unions.

In conclusion, we appreciate the FSB's focus on cyber incident reporting and appreciate the gravity and importance of the issues addressed by the consultation. We greatly appreciate the opportunity to comment on the FSB's **Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting.** Should you have any further questions, please feel free to contact me at aprice@woccu.org or +1 850-766-5699.

Sincerely,

Andrew T. Price
Sr. Vice President of Advocacy/General Counsel
World Council of Credit Unions