AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Brussels, November 2023

Dear European Supervisory Authorities (ESAs),

The American Chamber of Commerce to the EU (AmCham EU) appreciates the work undertaken by the ESAs regarding the Regulatory Technical Standards (RTS) on the classification of information and communication technology (ICT) incidents. However, the ESAs' inclusion of sharing incident reports across numerous authorities and on a non-anonymised basis will cause significant concerns for financial entities.

Incident reports constitute confidential security information for financial entities, possibly including technical details concerning an entity's IT infrastructure, IP addresses and information concerning vulnerabilities. These will be provided, in varying degrees of detail, across all respective forms of incident report (initial, intermediate and final) within the Digital Operational Resilience Act (DORA). Sharing this level of sensitive information across numerous authorities and on a non-anonymised basis creates a material cybersecurity risk for financial entities and will likely become a target for malicious actors. This requirement should not be included within the RTS. Rather, incident reports should only be shared on a need-to-know basis, with all sensitive information redacted where possible and, at a minimum, anonymised in all circumstances. Financial entities should, additionally, be informed of any other authorities that receive an incident report.

The cybersecurity risk faced by sharing incident reports is further exacerbated by the inclusion of other authorities outside of financial regulators within the RTS. The RTS states that incident reports would be shared to law-enforcement authorities, resolution authorities, NIS2 authorities at a national level and DORA authorities at a national level. A proliferation of authorities being included, alongside a decision to non-anonymise and share all incident report information, greatly increases the cybersecurity risk to financial entities. While the RTS states that the exchange of information will be shared in a secure manner, a financial entity would be unaware who has received their incident information (with detailed vulnerabilities included), what security practices those authorities have and how those authorities are using the information included. These factors are further amplified due to the increased risk of malicious actors targeting this information. Financial entities respectfully disagree that the RTS's proposal does not pose a threat to the security of the information.

Given the content of the information in incident reports has yet to be concluded, or consulted upon, the onward sharing of incident reports across such a wide variety of authorities within the EU should be removed. Additionally, the RTS is equally vague concerning what threshold will be used to share across authorities and what level of information is necessary to reduce the 'risk of contagion'. The risk of contagion constitutes a significant incident and is unclear regarding why all incident reporting information would need to be shared. This requirement would likely cause financial entities to be more cautious in choosing to send incident reports, likely reducing any proactive reporting and delaying incident reporting in practice. In order to build an effective reporting regime that encourages proactive participation by financial entities, the sharing regime should only be on a need-to-know basis, redacted where possible, anonymised and inform financial entities which authorities have

received their information. Finally, sharing beyond authorities should be done on an exceptional basis only.

AmCham EU stands ready to provide concrete proposals and contribute to the successful implementation of DORA. Please do not hesitate to reach out if you have any question or would like to discuss the issue further.

Best regards,

AmCham EU