8 April 2025

Homeland Security Group
Home Office
5th Floor, Peel Building
2 Marsham Street
London
SW1P 4DF

RE: Comments of the ACT | The App Association, *Ransomware Legislative Proposals Consultation*

ACT | The App Association writes to provide input to the Home Office in response to its consultation on legislative proposals to reduce ransomware payments to cyber criminals and increase incident reporting.[1]

The App Association represents thousands of small business innovators and startups in the software development and high tech space located in the United Kingdom and around the world.[2] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives, which today represents an economy worth more than $1.6 trillion annually and that provides millions of jobs around the world.[3]

We applaud the Home Office's efforts and commitment to obtaining input from a diverse set of stakeholders, especially from the small business community, in the development of its approach to implementing the cyber incident and ransom payment reporting requirements.

Cyber incident notification requirements could impose serious obligations on the broader business community and on small businesses in particular. **In its legislative proposals, the App Association urges the Home Office to prioritise the following:**

Establishing an appropriate reporting timeline. The regulation should reflect an appropriate, flexible standard for notifying government about significant cyber incidents.

[1] https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals.

[2] ACT | The App Association, *About*, *available at* http://actonline.org/about.

[3] ACT | The App Association, *State of the U.S. App Economy: 2022*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf

Covered entities may appropriately need to delay reporting if such reporting would disrupt an ongoing criminal or national security investigation, and reporting requirements should provide for such a delay when appropriate. Further, much may be discovered outside of the 72-hour timeframe after a cyber incident, and covered entities may need time to investigate an intrusion further, and to supplement an incident report. Covered entities should be given the ability to supplement a cyber incident, without penalty, after conducting initial mitigation and response efforts.

Appropriately scoping a reportable ransomware incident and who must report cyber incidents. Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed ransomware incidents. The definition of a covered cyber incident should be based on clear and objective criteria and should clearly differentiate between mere vulnerabilities and successful attacks that have caused harm. Any definition of a covered cyber incident that merits reporting should be limited to an incident that has a significant disruption to critical infrastructure operations. Reporting obligations should be extended only to companies that manage risks and disruptions to critical infrastructure, and size-based criteria that make the legislation's coverage debilitatingly large should be avoided.

Clarifying the key elements of an incident report. A cyber incident report should feature information such as how the attack was discovered; the vulnerability exploited and what metrics indicated the attack's success; what steps, if any, have been taken to mitigate the attack; and what the known impacts of the attack are. We encourage the Home Office to eliminate onerous reporting requirements and limit required detail of initial reports to facilitate faster reporting and reduce security risk.

Providing needed liability protections. The Home Office should establish that the act of reporting a covered incident and the contents of any report, including supplemental reporting, do not unnecessarily subject a covered entity to discovery in any civil or criminal action, which would ultimately chill the public-private partnership construct needed for timely and appropriate cybersecurity incident reporting and collaborative efforts to mitigate harmful cyber incidents. Reporting entities, in essence, should not be penalised after the fact for complying with a legal obligation. In addition, we urge the Home Office to tailor the amount of information that covered entities would be required to submit to the elements necessary to achieve the proposed legislation's goals. There must be a compliance regime that treats cyberattack victims as victims, with a reporting program that encourages cooperation and strengthens trust between the public and private sectors. A regulatory-based approach that focuses on punitive actions, such as penalties rather than mutual gains would run counter to the goal of creating a strong national partnership model to address the increasing cyber threats facing the United Kingdom.

Reporting to a victim entity or its designee, including an information sharing and analysis organization or center, should generally be limited. Cyber incident response service providers, such as cybersecurity firms, law firms, and insurers, should not be required to report incidents to government entities that have occurred on their

customers' networks unless explicitly authorised by their customers to do so on their behalf. This approach would avoid unintended outcomes like compelling cybersecurity providers to disclose clients' sensitive business information in breach contractual obligations and/or dissuading businesses from employing outside experts to the detriment of businesses' cyber defenses.

Educating and partnering with the innovation community. Many in the app developer community face significant resource constraints as they operate in supply chains across critical sectors. The Home Office's partnership and resources will be critical to outreach, awareness, and education for these entities subject to new proposed reporting requirements, particularly small businesses, and proposed legislation should include a robust education and support campaign focused on these entities.

ACT | The App Association appreciates the opportunity to provide input to the Home Office on the importance of cyber incident and ransom payment reporting and looks forward to continued collaboration.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005