On January 5, 2018, the U.S. Secretaries of Commerce and Homeland Security published a "DRAFT FOR PUBLIC COMMENT" on Executive Order 13800, "Enhancing the Resilience of the Internet and Communications Eco-Systems Against Botnets and Other Automated, Distributed Threats."[1]

The draft highlights the risks posed by ever-increasing botnets in size and speed of attacks. Insecure, and thus dangerous, IOT devices are being installed in homes and businesses on every continent and are expected to outnumber mobile phones in 2018. Aligned under 5 goals, the Draft proposes 23 actionable steps that should be taken by government and industry to move the botnet acceleration needle in the other direction.

The A-ISAC believes this report is a well-thought-out document and we commend the inclusion of actionable steps toward significantly reducing the impact of botnets. The calls to action underscore the importance that every company must understand its role in the shared risk of enabling the existence of botnets. Aviation companies, like those in all sectors, play many roles in the digital eco-system that supports botnets: as the purchasers of IOT devices, in configuring networks, addressing vulnerabilities, and in product design and development.

Since our inception, the A-ISAC has espoused the concept of shared risk reduction. For example, both airlines and airports can be significantly impacted if one or the other becomes incapacitated due to a cyber-attack. Similarly, bot enabled attacks on aviation supply chains, global aviation communications networks and more, have the potential to cause a significant ripple effect. The report emphasizes, and we support, the need for sector-wide information sharing despite the disparity in cyber capability of companies within the sector. Many companies have well-funded, mature cyber programs but thousands more are underfunded/understaffed in their cyber security functions.

In the decade leading up to 1970, hijackings were out of control. In 1969 there were 87 hijackings worldwide and 40 of those in the United States. In 1970, the United States drew the line and began to screen passengers for weapons. Similarly, there have been enough botnet attacks to motivate us to act now to promote that all digital products be secure. We need the ability to screen for and identify malicious internet traffic. The solution must be multifaceted, from ISPs to companies making and buying IOT devices. Innovators must accept the responsibility to slow their race to the market and focus on delivering more secure digital products.

The Executive Order is looking for ways to incentivize security. Independent researchers will continue to find errors in coding. We applaud researchers who work with companies under the model of responsible disclosure, thus giving the software development company time to issue a patch ahead of global awareness of the vulnerability. Looking ahead, market forces will likely drive litigation against companies for coding errors which resulted in vulnerabilities proven to be the root cause for loss due to a cyber-attack. We recommend consideration to limit liability to companies who make swift public disclosures of vulnerabilities and expeditiously issue patches. This will incentivize two key pillars in reducing cyber risk: the independent researchers will be motivated to continue notifying companies of coding errors and companies will be incentivized to respond quickly. This will drive companies to stay abreast of the

[1] https://csrc.nist.gov/publications/detail/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-president/draft

security of their products and prioritize a steady state of security for products they have released to market.

Goal 3 in the draft addresses the future: “Promote innovation at the edge of the network to prevent, detect and mitigate bad behavior.” As a global critical infrastructure, the Aviation Sector is poised to lead efforts in support of this goal. We intersect at many points with government infrastructures that manage air traffic controls, airports, and defense airspace. The Aviation ISAC is rapidly growing and already has in place a worldwide network for aviation companies across the entire aviation eco-system to share critical intelligence information.

The A-ISAC highlights the importance of Goal 4’s Action 4.5 “The cybersecurity community should continue to engage with the operational technology community to promote awareness and accelerate cybersecurity technology transfer.” Within the aviation industry, the OT and IT communities are on the cutting edge of innovation in safety and cyber security. We will continue to support and encourage the exchange of best practices in product development and design within our sector and across sectors.

The draft is a call to both industry and government to drive the pillar of security into the exploding IOT industry. We wholeheartedly support and endorse this effort and global exchange of best practices in our sector and among all sectors to continue to make the global aviation market safe and resilient.