Charter of Trust response to the US Executive Order 14208 – Improving the Nation's cyber security

In May of 2021, the Biden administration made a significant commitment to address the persistent and growing cyber threat by issuing Executive Order 14208 - Improving the Nation's Cybersecurity "EO". The EO is a comprehensive whole of government approach and significant partnership with industry to establish comprehensive framework for new requirements in key areas, including:

- Software supply chain security requirements for software sold to the federal government
- Enhanced threat information sharing between government and the private sector
- Federal IT modernization, including accelerated adoption of cloud technology and enhanced security requirements for cloud, and zero trust architecture

The Biden Administration says: "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy" signaling that the initiatives in the EO to advance resiliency will be suggested best practices not only for US companies, but across major corporations globally.

Reflecting on the past year, the rate of cyber-attacks has only accelerated, with vulnerabilities like Log4j demonstrating the importance of supply chain security. Like the administration, Congress also responded by passing, the Cyber Incident Reporting for Critical Infrastructure Act as a sharing regime to garner greater insight about cyber threats and patterns and enhance collaboration with the private sector to prepare and ultimately prevent incidents from occurring.

Founded in 2018, The Charter of Trust is a multinational organization of 17 partners with the goal of jointly shaping cybersecurity through a trusting relationship among society, political leaders, business partners and customers. Aligned to our global complexities and interdependencies, the Charter of Trust is committed to developing ways to bolster the lines of defenses that protect supply chains and critical infrastructure through 10 core principles[i] that build trust in digital technologies. Of the 10, three in particular support the key areas of the EO highlighted above:

- **Principle 2 – Responsibility throughout the digital supply chain**
    - Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as identity and access management, encryption and continuous protection.

- **Principle 3 – Security by default**
    - Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.

- **Principle 8 - Transparency and response**
    - Maintain and expand a network of experts who share new insights and information on incidents to foster collective cybersecurity; engage with regulators and other stakeholders on threat intelligence sharing policy and exchange best practices.

The Charter of Trust applauds the administration for their herculean effort to drive practices to improve security through government and industry collaboration on very challenging business operation topics in order to affect change and garner greater visibility and resilience. The members of the Charter of Trust look forward to the next year and the implementation of the EO practices and stand ready with our principles to find innovative ways to get to the same goal globally.

---

[i] https://www.charteroftrust.com/about/