SUMMARY BRIEFING

# Executive order on improving the nation's cybersecurity

1898 & CO.
PART OF BURNS & MCDONNELL

## SUMMARY

On May 12, 2021, President Biden issued an Executive Order (EO) aiming to improve the federal government's efforts to "**identify, deter, protect against, detect and respond**" to cybersecurity incidents.

Released five days after the ransomware attack on Colonial Pipeline, it is intended as a comprehensive response to an **ongoing trend of increased threats**.

The EO is intended to help the government modernize and mitigate the risk of cyber incidents. It also aims to **encourage private-sector-owned domestic critical infrastructure to partner with and follow the federal government's lead** to take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents.

The EO required quick action, with 30-day, 90-day and 365-day deadlines across seven key objectives.

**The mission of the 1898 & Co. cybersecurity team is to serve humanity by improving the safety and reliability of the world's critical infrastructure. We do this by improving risk management through resiliency, improved situational awareness and preparedness.**

**For more information, visit 1898andCo.com/services/manage-your-risk.**

***Please review our cybersecurity services and don't hesitate to reach out with any questions.***


**Carmen Garibi**
carmen.garibi@1898andco.com

**Marco Ayala**
marco.ayala@1898andco.com

**Matt Morris**
matt.morris@1898andco.com


1898 & CO℠
PART OF BURNS & MCDONNELL

# OBJECTIVES

## Remove barriers to threat information sharing between government and private sector

- Propose **new contract language** for IT and OT service providers whose current contract terms may restrict the sharing of cyberthreat or incident information with the federal government.
- Define and clarify cyberthreat and incident **reporting policies** depending on level of severity and type of attack, while identifying protection for privacy and civil liberties.

## Modernize and implement stronger cybersecurity standards

- Moves the government to secure cloud services and a zero-trust architecture.
- Mandates the deployment of multifactor authentication and encryption.

## Improve software supply chain security

- In partnership with private sector, academia, and other appropriate actors, the federal government will identify and publish preliminary guidelines — standards, tools, and best practices — and complete periodic reviews for development of software sold to the government.
- Requires developers to maintain greater visibility into their software and make security data publicly available, including providing a Software Bill of Materials (SBOM) for each product, either directly or by publishing it on a public website.
- Stands up a concurrent public-private process to develop new and innovative approaches to secure software development and uses the power of federal procurement to incentivize the market.
- Creates a pilot program to create an "Energy Star" type of certification for software that was developed securely.

## Establish a cybersecurity safety review board

- Includes representatives from the DoD, DoJ, CISA, NSA, FBI and from private-sector cybersecurity or software suppliers as determined by DHS.
- Will review and assess threat activity, vulnerabilities, mitigation activities and agency responses.
- Will convene as needed following a significant cyber incident, triggering the establishment of a Cyber Unified Coordination Group.

## Standardize a cybersecurity vulnerabilities and incident response playbook

- All federal agencies will respond using a unified approach, rather than the current varied response processes.

## Improve detection of cybersecurity vulnerabilities and incidents

- Employ resources to maximize early detection, like those available through 1898 & Co. **Managed Threat Detection and Response**.
- Deploy an **Endpoint Detection and Response** (EDR) initiative.

## Improve investigative and remediation capabilities

- **Deploy standard requirements for logging of events** and other relevant data retention.

25084-0721