A Brief Analysis of the May 2021 Cybersecurity Executive Order

In response to the recent ransomware attack on Colonial Pipeline, the Biden administration recently issued an Executive Order on "Improving the Nation's Cybersecurity." The document addresses a series of ongoing cybersecurity concerns both directly and indirectly brought to light by the Colonial Pipeline incident. This Executive Order places a large emphasis on intelligence sharing and improved cooperation between the public and private sectors to better detect and respond to cybersecurity incidents — bringing together key stakeholders as well as allies to defend the United States from cyber threats.

Although wide-ranging in its proposed impact areas, the Executive Order focuses on five key strategic initiatives:

- **Accelerate threat intel sharing between the public and private sector**
- **Modernize cybersecurity standards within the Federal Government**
- **Improve security within the software supply chain**
- **Establish the Cybersecurity Safety Review Board**
- **Standardize cyber incident response playbooks and improve incident detection and response capabilities**

Accelerate Threat Intel Sharing Between The Public and Private Sector

Via this Executive Order, the Federal Government has committed to proposing an overhaul of current contractual terms that restrict threat or incident intel sharing with government contractors — specifically calling out Cloud Service providers. This will likely be a slow moving process as it will require both existing contract cycles to expire and some of the largest IT, Operations, and Cybersecurity providers to agree to share security information.

Several states have already begun similar programs targeted towards accelerating and growing threat intelligence sharing programs in cooperation with the private sector. One such example is the Multi-State Information Sharing and Analysis Center (MS-ISAC) sponsored by the Center for Internet Security (CIS), which includes participation from Arizona, Louisiana, Massachusetts, and Texas among others [(1)]. The Federal Government's move to prioritize private-public threat intelligence sharing is a key step in removing some of the obstacles in our nation's cybersecurity sector that slow down or even halt information flow among key stakeholders and allies.

Modernize Cybersecurity Standards Within the Federal Government

A key component of the Federal Government's proposal to modernize their own cybersecurity capabilities and standards is a direct call to move towards a Zero Trust Architecture. The order advises leveraging existing standards as documented by the National Institute of Standards and Technology (NIST) and collaboration with cloud providers for government services using SaaS, IaaS, or PaaS technologies [(2)]. The move toward Zero Trust Architecture will likely require massive modernization efforts in identity and access management to ensure well defined roles and privileges for the government's operational resources and IT assets.

Zero Trust Architecture is a popular choice in modern IT environments with the expansion of the “perimeter” and internet-connected infrastructure. As both the public and the private sector increasingly transition to cloud-based solutions, identity and access management will be key to limiting cybersecurity threats and providing better controlled IT resources.

Improve Security Within the Software Supply Chain

This section of the Executive Order focuses on the supply chain — and, more broadly, on improving security resiliency with Third Parties and Vendors. The software development lifecycle and modernization efforts to better integrate security into product development (“DevSecOps” or “Moving Security to the Left”) are becoming more and more mature functions in the private sector for IT and product development organizations. However, vendor and third party software, tools, and applications can be a black box without proper reviews and an understanding of the key tests, checks, and gateways that their security teams build into the product.

Establishing clear third party vendor risk standards for government contractors, suppliers, and partners will improve security throughout the private sector since many private enterprises also use these service providers and tools. Earlier identification of security risks and vulnerabilities can lead to earlier security remediation efforts and fewer security incidents.

Establish the Cybersecurity Safety Review Board

By leveraging its power to convene public and private sector leaders in a review board, the Federal Government is attempting to provide overarching leadership during cybersecurity incidents that may affect both public and private sector infrastructure, systems, or assets. Currently, incident response teams are often limited to key stakeholders within the affected organization, which does not necessarily provide the scale or resources that a broader response group may be able to offer.

In tandem with the efforts to increase threat intelligence sharing, this Review Board puts cooperation and coordination at top of mind for cybersecurity practitioners from all sectors and provides a pathway to leveraging resources from the Federal Government to respond to all types of cyber incidents.

Standardize Cybersecurity Incident Response Playbooks and Improve Incident Detection and Response Capabilities

The Federal Government is following along with efforts by many State and Local Governments to harden, improve, and optimize cybersecurity incident response plans. Many smaller government entities have already begun the process of contracting out for cybersecurity professionals to review, improve, and modernize response plans that likely were not developed to suit the current IT environment, technologies, or threats. Leveraging a shared set of baselines, standards, and processes can help the federal government quickly and effectively react to cybersecurity incidents at all levels of government and provide efficient support to the private sector as needed.

Improving the detection and response capabilities to cybersecurity incidents is a clear siren call from the Colonial Pipeline ransomware attack in addition to several high profile cybersecurity incidents over the past few years. These incidents not only highlight resource and technology constraints, but also the limitations of government capabilities to prevent attacks and mitigate the damage once they occur. Improved capabilities also significantly benefit the private sector as these cybersecurity incidents are rarely contained to just one attack vector, often using the connected infrastructure of many systems.

Closing Thoughts

This Executive Order is a key step in accelerating efforts to improve the cybersecurity posture of Federal, State, and Local Government. In addition, it fosters innovation and resiliency within the private sector. As our infrastructure becomes more interconnected and dependent on key networks, systems, and stakeholders, it will be a significant undertaking to ensure consistency across baselines and standards for a more cybersecurity resilient nation.

(1) Center for Internet Security - MS-ISAC https://www.cisecurity.org/ms-isac/
(2) Software as a Service, Infrastructure as a Service, Platform as a Service

Sources:

- *Executive Order on Improving the Nation's Cybersecurity. May 12, 2021. Presidential Actions*
- *Fact Sheet: President Signs Executive Order Charting New Course to Improve Nation's Cybersecurity and Protect Federal Government Networks. May 12, 2021. Statements and Releases*

DAYBLINK

For any questions or comments on the analysis above, or any of the cybersecurity materials found on the DayBlink website, please contact:

Michael Morgenstern, Partner *(Michael.Morgenstern@dayblink.com)*
Justin Whitaker, Partner *(Justin.Whitaker@dayblink.com)*
Jacob Armijo, CISM, Manager *(Jacob.Armijo@dayblink.com)*