# Biden signs Executive Order on Improving the Nation's Cybersecurity

5.13.2021

President Biden executed the much-anticipated Executive Order [1] on cybersecurity yesterday, highlighting the growing prevalence of cyber attacks and increasing concerns about the impacts these attacks have had on the public and private sectors and Americans' security and privacy. This comes at a time when threat actors are becoming increasing sophisticated in the scope and breadth of their attacks. We need no better example than the DarkSide attack on Colonial Pipeline last week.

The President's EO had been expected for several months and includes details and timelines that are beyond the scope of this preliminary Alert. We will follow up with further commentary as the notices appear in the Federal Register. For now, we have outlined its basic provisions:

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector
  - The goal is for government service providers, "to the greatest extent possible," share cybersecurity incident data "as may be necessary" for government agencies to respond to "cyber threats, incidents, and risks"; the focus here is on removing the contractual barriers that currently impede or prevent service providers from sharing incident data with the government
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government
  - Outdated security models (on-premises) and unencrypted data have left both private and public sectors vulnerable; establish training programs
- Improve Software Supply Chain Security
  - Encourage security by design and create an "energy star" type of label for software that has been developed in a secure fashion

## Related Services

Cybersecurity and Privacy Specialty Team

- Establish a Cybersecurity Safety Review Board
  - Modeled after the NTSB and designed to ask the hard questions when a significant cybersecurity incident occurs
- Create a Standard Playbook for Responding to Cyber Incidents
  - The EO calls it a Standard Playbook, but the analog in the private sector is an Incident Response Plan
- Improve Detection of Cybersecurity Incidents on Federal Government Networks
  - Endpoint detection and response (EDR) that will detect and mitigate malicious cyber activity
- Improve Investigative and Remediation Capabilities
  - Establish requirements for logging events and retaining relevant data

After reading this EO, it was interesting to note the parallels to what those of us in private industry consulting have advocated for years as "best practices." Because of the critical importance of maintaining both a secure IT (information technology) and OT (operational technology) environment, we have distilled these basic best practices below:

- Implement multifactor authentication (threat actors thrive when MFA is not deployed)
- Mandate Virtual Private Networks (VPNs) for remote access to company networks (critical for a dispersed and/or work-from-home workforce)
- Deploy endpoint detection and response (EDRs will detect and prevent most incidents automatically and do so 24/7/365)
- Implement Incident Response Plans (without a plan, it can be chaos)
- Encrypt confidential and sensitive data both at rest and in transit (encrypted data is useless to threat actors and a non-event under most data breach laws)
- Back up data (encrypted) and secure that backup off-site (with a good backup available, no ransom payment is necessary)
- Turn on logging (you can't find what you can't see)
- Segment data across IT networks (don't make it easy for threat actors to crawl across your network)
- Control access credentials to need-to-have individuals (threat actors target IT managers with the "keys" to the network)
- Implement periodic training for all (training works and it's simple to do)
- Purchase a comprehensive cyber insurance policy (and pre-vet your cyber counsel and forensic team)
- Maintain physical security controls (lock your doors and lock up your sensitive equipment)
- Conduct periodic external and internal vulnerability scans (security is not a one-and-done effort and requires constant vigilance)

The point is this: if the above practices were implemented company-wide, the rate and impact of cyber attacks would be reduced markedly. There may be costs associated with their implementation, but the costs of non-implementation are much higher.

For over fifteen years we have been counseling clients on cybersecurity, and each item from the list of best practices above has a story to tell and a lesson learned. We would be pleased to offer our advice and counsel in a preventative mode, as opposed to reactive, but we are prepared for both.

**Claudia Rast**
734.213.3431
rast@butzel.com

**Ira Hoffman**
202.454.2849
hoffmani@butzel.com

**Jennifer Dukarski**
734.213.3427
dukarski@butzel.com

**Debra Geroux**
248.258.2603
geroux@butzel.com

**Ashley Glime**
734.213.3631
glime@butzel.com

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/