Lazarus Alliance
Proactive Cyber Security©

A Sea Change in Security: Federal Defense Systems, Vulnerabilities and President Biden's Executive Order on Cybersecurity

On May 12, 2021, President Joseph Biden issued Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity." This long called-for order followed years of increasingly complex and pervasive threats to the nation's IT infrastructure. The White House emphasizes several real and ongoing challenges that federal and defense agencies face in terms of cyberattacks. More importantly, this document acknowledges the reality that cyberwarfare is quickly becoming the norm, and the face of that battlefield will look quite different than conflicts of the past.

This whitepaper will cover some of the details of this Executive Order, including what it means for businesses that want to work with federal and defense agencies in the future.

What is Executive Order 14028?

This executive order was written and executed to address, as per the language of the document, the "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector and ultimately the American people's security and privacy."

This is a sweeping statement of purpose, but it speaks to the unique and challenging times we face. State-sponsored cyber warfare has been an ever-growing problem for decades. Still, the prevalence of networked and connected systems and online access to documents and system resources have only exacerbated the issue. Furthermore, the emergence of COVID-19 and the subsequent move to remote work and decentralized data access have presented malicious cybercriminals with more opportunities than ever to undermine IT security.

Following all of these issues, we have seen an uptick in significant data breaches and thefts through technologies like malware, ransomware and Advanced Persistent Threats (APTs). Some of these attacks include:

- **SolarWinds (2020)**: An undetected hack into the patching and updating mechanisms of SolarWinds's Orion network monitoring and management system led to the compromise of their cloud systems, both internally and those of their numerous clients. Unnoticed for months, the breach affected dozens of private and public organizations, including Microsoft, FireEye, the Department of Homeland Security, and the Pentagon.

- **Numerous Telecommunication Companies (2021):** A Chinese hacking group was linked to a breach of calling and text records from at least 13 telecommunication providers.

- **Microsoft (2021):** At the beginning of March, Microsoft admitted publicly that a Chinese group attacked and breached Microsoft Exchange servers responsible for handling emails for subscribers. This breach potentially affected 30,000 client organizations.

- **Colonial Pipeline (2021):** Russian hackers attacked the IT infrastructure of Colonial Pipeline and locked critical system data behind ransomware. While the hack was not specifically claimed as state-sponsored, it was driven by the importance of Colonial Pipelines to U.S. energy concerns.

EO 14028 specifically cites incidents like these as the reasoning for its publication. The reality is that malicious hackers are leveraging the fact that U.S. infrastructure, both public and private, is built on sensitive cloud environments supported by a digital supply chain by which most, if not all, major organizations in the country are connected.

What Cybersecurity Measures Does EO 14028 Require?

The primary goal of this EO is to modernize U.S. cybersecurity. As such, it identifies a few significant gaps in our capabilities:

- **Public vs. Private Distinctions**: The federal and defense supply chains aren't monolithic nor built entirely inside or outside the government. Third-party vendors offering security, cloud, SaaS, and infrastructural services support the functionality of most government organizations. Furthermore, major private businesses in industries like energy production, manufacturing, and supply chain logistics--all critical to the operation of the U.S. economy--share many of these same IT vendors with government agencies.

We then see a perfect storm where public and private infrastructure overlap, and a threat against one serve as a potential domino for continuing threats against all.

- **Organizational Communication**: Information about breaches, hacks and security issues are often siloed behind different sets of bureaucracies (public and private). Information ironically doesn't move that fast these days. For example, the SolarWinds hack was originally written about by FireEye, a security firm using the Orion platform but otherwise associated with SolarWinds.

  Furthermore, there are no direct requirements for companies to report breaches promptly, either to the government or the public.

- **Standardization of Cybersecurity**: Standards and regulations exist, surely, and organizations like the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) publish cybersecurity guidelines that, in part or whole, end up informing national security standards like FedRAMP, CMMC and the NIST Cybersecurity Framework (CSF) and Risk Management Framework (RMF).

  However, the standards contained within these frameworks are disparate, piecemeal. One framework might implement some of the requirements of NIST SP 800-53, while another calls for ISO 27001 compliance. Others might take parts of these and implement them based on best practices as determined by governing bodies.

  Unfortunately, the issue is that there is still a level of fragmentation with this approach, especially across private and public institutions.

Based on these technical realities, the EO calls for several different upgrades to cybersecurity:

1. **Zero-Trust Security:** Zero-trust infrastructure simply means developing access and authentication controls that do not assume that any user, device, or request is trustworthy. As such, system authorization mechanisms should challenge every request. This approach isn't necessarily widespread, and the EO calls for universal implementation of zero-trust principles for government agencies and contractors.

2. **Software Bill of Materials:** Organizations in the supply chain must define and catalog their technologies, including software, hardware, and other technical products, as part of a Software Bill of Materials (SBOM). This includes IoT and cloud technologies and anything managed or attached to third-party vendors.

3. **The Cyber Safety Review Board:** Section 5 of the EO directs the Secretary of Homeland Security to develop a Cyber Safety Review Board with the express purpose of reviewing federal and supply chain systems, threat activities and response/mitigation protocols. This board will also convene during security events to coordinate responses.

4. **The Federal Government Playbook:** Within 120 days, the Secretary of Homeland Security shall consult with CISA, OMB and Chief Information officers to build a standardized cybersecurity playbook based on NIST standards.

5. **Response and Remediation:** Homeland Security, CISA and OMB are tasked with ensuring that all resources necessary to respond to security events and remediate issues immediately are available.

What is the Impact on Vendors Working in the Federal Supply Chain?
The short answer is that not much is known about the trickle-down effect of this EO.

Some of the more concrete aspects of the order (implementing zero-trust architectures) will surely come into play sooner rather than later. Others, like a centralized playbook and remediation efforts, will rest on the decision made by the various defense and security departments, NIST and regulatory bodies.

For the most part, private companies working with government and defense agencies will see changes occur in the existing compliance requirements they already adhere to. Changes to frameworks like FedRAMP and CMMC will most likely reflect any changes to their underlying requirements.

The truth, however, is that the changes may be so esoteric and specific that focusing on them can distract you from the job of growing your business and serving clients.

Lazarus Alliance
Proactive Cyber Security©

Lazarus Alliance: Navigate Evolving Government Cybersecurity Requirements

Times are changing, and the requirements that companies like yours will take up to support your clients are also changing. Despite what many in the private sector might think, this is for the better. As the landscape of modern cyberwarfare shifts, so too must our responsibilities.

Lazarus Alliance supports businesses and other organizations by streamlining compliance effectively without sacrificing security. Even the simplest audits have historically taken weeks or months… a painful and resource-intensive process that many businesses undergo annually or even quarterly. With Lazarus Alliance, you can take these complex processes and reduce time invested to days or even hours.

We work with organizations inside and outside the federal supply chain. Our expertise extends to several of the most complex and pervasive compliance standards around, including:

1. HIPAA and HITECH
2. FedRAMP
3. StateRAMP
4. EUCS
5. C5
6. CMMC
7. GDPR
8. PCI
9. IRS 1075
10. SOX
11. NIST 800-53
12. DFARS NIST 800-171
13. The ISO 27000 Series
14. SEC, NFA and FINRA
15. Financial Audits
16. CCPA

And more.

If you want to take control of your compliance and audits, streamline security implementation and stay ahead of changing standards without derailing critical business processes, then contact Lazarus Alliance for a consultation.

Lazarus Alliance is Proactive Cyber Security©

In any jurisdiction, and in all industries, we are your global partner in compliance, risk, policy, security testing, financial audit and Cybervisor© services.