IMPROVING THE NATION'S CYBERSECURITY

AN ICIT FELLOWS' ANALYSIS OF PRESIDENT BIDEN'S EXECUTIVE ORDER

JUNE 2021

Authored By:
Drew Spaniel, Lead Researcher, ICIT
Joyce Hunter, Executive Director, ICIT

Contributors Include:
David Wray, ICIT Fellow & CTO, Micro Focus Government Solutions
Jim Routh, ICIT Fellow & Advisor, Board Member, & Former CSO
Don Maclean, ICIT Fellow & Chief Cybersecurity Technologist, DLT
Itzik Kotler, ICIT Fellow & Co-Founder & CTO, SafeBreach
Parham Eftekhari, ICIT Founder & Chairman & Executive Director, Cybersecurity Collaborative
Michal Aisenberg, ICIT Fellow & Chief Cyber Policy Counsel, MITRE
Dr. Barry West, ICIT Fellow & Former Acting CIO, DHS
Stan Mierzwa, Director, Center for Cybersecurity, Kean University
Kevin Hansen, CTO, Federal Channels & Alliances, Micro Focus Government Solutions

ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Contents

Overview

President Biden's Executive Order on *Improving the Nation's Cybersecurity* calls for ambitious cybersecurity reform across the federal space in response to recent incidents such as the attacks against SolarWinds and the Colonial Pipeline. Jim Routh, ICIT Fellow and Former Mass Mutual CSO, opines, "This Executive Order represents an essential and positive step forward for the nation's cyber resilience capabilities" because he expects the impact of the Executive Order (EO) to be a positive re-affirmation of the importance of cyber resilience to the nation and enterprises. The Executive Order states: "This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person." However, it does institute binding directives for the federal agencies' cybersecurity practices and acquisition processes. ICIT believes that over time the directives set by the Executive Order will catalyze cybersecurity reform within private contracting companies that will then propagate to the private sector overall. As best practices normalize, security across all critical infrastructure sectors will holistically improve.

The Executive Order promises more comprehensive and broad cybersecurity reforms than those introduced by prior administrations. Dr. Barry West, ICIT Fellow and Former Acting CIO, DHS, participated in creating and executing Executive Order 13800 in May 2017. He proffers that "[EO 13800] did a good job of getting some momentum around high-value assets and ensuring agency heads were held responsible for Cybersecurity and not just the CIO and CISO. But, it did not touch on other key areas we now see in this new Executive Order." Some of those critical areas include:

- Supply Chain is vital. It is crucial to hold organizations in public and private sectors responsible for secure software development and ensure that security standards apply to all vendors and third parties that participate in development.
- Better collaboration between the public and private sectors; Having a Review Board co-chaired by both the public and private sector stakeholders should increase awareness and foster better communications.
- A standard playbook will yield significant impacts both in the short-term and long term. In addition, this will allow organizations to have one standard for incident response.

Key Tenets of the Executive Order on Improving the Nation's Cybersecurity

Threat Information Sharing

The Executive Order ensures that IT Service Providers can share information with the government and requires them to share certain breach information. However, IT providers are often hesitant or unable to share information about a compromise voluntarily. Sometimes this can be due to contractual obligations; in other cases, providers may be reluctant to share information about their own security breaches. Removing any contractual barriers and requiring providers to share breach information that could impact Government networks is necessary to enable more effective defenses of Federal departments and holistically improve the Nation's cybersecurity [1] [2].

The Executive Order states that IT service providers, including cloud service providers, have contract terms that may prevent the sharing of cyber threats or information on federal information systems. By July 11, 2021, the EO requires the Office of Management and Budget, in consultation with other named federal agencies, to make recommendations for contract language changes, including:

- Updating descriptions of contractors and covered entities;
- Requiring service provider to collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies' requirements;
- Recommending that service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies;
- Incentivizing service providers to collaborate with Federal cybersecurity or investigative agencies to investigate and respond to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed.

Proposed changes to the Federal Acquisition Regulation (FAR) will be published by November 8, 2021.

Cyber Incident Reporting

Government contractors that provide software or services would be required to report cyber incidents to the relevant federal agencies based upon a sliding scale of risk assessment, with the highest risk requiring notice within three days of discovery. In addition, the Executive Order standardizes the definition of "incident" to that of 44 U.S.C. § 3552(b)(2):

> (2) The term "incident" means an occurrence that—
>
> (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
>
> (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

By June 28, 2021, the Department of Homeland Security, in consultation with other named federal agencies, is directed to recommend changes to the FAR, including the nature of the cyber incidents that would require reporting, the government contractors and service providers that would be covered, the periods for reporting based on "a graduated scale of severity," and "appropriate and effective protections for privacy and civil liberties." By September 27, 2021, the FAR Council will publish the proposed FAR updates for public comment. Additionally, by July 11, 2021, the FAR Council will begin assessing the cybersecurity requirements for unclassified systems contracts. The council will review and publish their recommended changes for public comment by September 9, 2021, for public comment.

Enhancing Software Supply Chain Security

The Executive Order will improve software security by establishing baseline security standards for the development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available. In addition, it 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.

By June 11, 2021, the Executive Order mandates the National Institute of Standards and Technology (NIST), in consultation with other named federal agencies, to solicit "input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria." In addition, by November 8, 2021, NIST is directed to publish preliminary guidelines for enhancing software supply chain security. The guidance

must include standards, procedures, or criteria, including multifactor authentication, encryption for data, "employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;" "providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;" and "participating in a vulnerability disclosure program that includes a reporting and disclosure process."

The Executive Order also creates a pilot program to create an "energy star" type of label so the government and the public can quickly determine whether software was developed securely. The initiative is similar to the Cyber Shield Act introduced by Representative Ted Lieu and Senator Ed Markey and endorsed by ICIT. This label would help prevent the federal government from acquiring critical software that was not designed with security controls throughout its development lifecycle. Especially for critical infrastructure systems, defense software, and other national security assets, negligently developed or intentionally vulnerable systems pose a significant risk of adversarial compromise or nation-state APT espionage. By adopting an assessment and labeling program, the Federal Government can leverage its considerable market power to drive software vendors to incorporate security into their products from the start of the development lifecycle and prioritize security and privacy controls at each stage. As a result, over time, security by design will normalize in the private sector according to the federal standard, and the culture overall will improve to protect consumers as much as the federal agencies.

Modernizing Federal Government Cybersecurity

Legacy systems pose significant risks to federal agencies since many systems are incompatible with secure software and hardware or are no longer supported with patches against emerging threats. Worse, legacy systems cost as much as four times modern systems to maintain. Outdated security models and unencrypted data have led to compromises of systems in the public and private sectors. Arguably, OPM, SolarWinds, and many major federal incidents are in part attributable to legacy infrastructure. The Federal government must lead the way and increase its adoption of security best practices, including employing a zero-trust security model, accelerating movement to secure cloud services, and consistently deploying foundational security tools such as multifactor authentication and encryption.

The Executive Order helps move the Federal government to secure cloud services and a zero-trust architecture and mandates the deployment of multifactor authentication and encryption [2]. Don Maclean, ICIT Fellow and Chief Cybersecurity Technologist, DLT, explains, "These measures are essential, especially in the wake of the recent Colonial Pipeline intrusion, an inept but ominous attack on a water treatment plant, and the highly sophisticated 'Sunburst' hack that affected private industry and public sector organizations, even including cybersecurity

firms. The Zero Trust mandate is particularly relevant. This concept, based on the sober-minded acknowledgment that intrusion is inevitable, has recently seen an enormous uptick in interest. It is time to re-think our defenses from the ground up, focusing on rapid and automated response, placing defenses as close to the target as possible, and focusing on mitigation as much as prevention. Zero trust and the other measures in this Executive Order are essential for improving America's cybersecurity. Executive Orders, however, do not always yield their intended result. The broad scope entails a commensurate budget, which is often lacking, and practical difficulties delay and undercut even the best plans. I hope agencies and contractors can meet the ambitious goals of this mandate. If so, we will have improved our nation's security" [3].

Establishing a Cyber Safety Review Board

Too often, organizations repeat past mistakes and do not learn lessons from significant cyber incidents. When security controls fail, or an incident occurs, agency stakeholders, the private sector, and the Administration need to investigate and critically evaluate the security paradigm to ascertain where and how a vulnerability was exploited and how to implement the necessary improvements to mitigate future compromise. The Executive Order establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leaders, that may convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity. This board is modeled after the National Transportation Safety Board, which is used after airplane crashes and other incidents.

Standardizing the Federal Government Cyber Incident Response to Incidents and Vulnerabilities

Organizations cannot wait until they are compromised to figure out how to respond to an attack. Recent incidents have shown that within the government, the maturity level of response plans varies widely. The Executive Order creates a standardized playbook and definitions for cyber incident response by federal departments and agencies. The playbook will ensure all Federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat. The playbook will also provide the private sector with a template for its response efforts [2].

Improving Federal Cybersecurity Vulnerability and Incident Detection

Slow and inconsistent deployment of foundational cybersecurity tools and practices leaves an organization exposed to adversaries. The Federal government should lead in cybersecurity, and strong, Government-wide Endpoint Detection and Response (EDR) deployment coupled with

robust intra-governmental information sharing are essential. The Executive Order improves the ability to detect malicious cyber activity on federal networks by enabling a government-wide endpoint detection and response system and improved information sharing within the Federal government [2].

Improving Federal Government Incident Detection, Response, and Remediation

Insufficient logging hampers an organization's ability to detect intrusions, mitigate those in progress, and determine the extent of an incident after the fact. Robust and consistent logging practices are invaluable practices to mitigate threats before adversaries can compromise critical assets or inflict harm. The Executive Order creates cybersecurity event log requirements for federal departments and agencies [2].

Foundations for Future Work

The Executive Order proposes robust reforms that, if executed effectively, could reshape national cybersecurity and lead to lasting reforms. However, ICIT fellows identified a few areas where the efforts set by the Executive Order could advance in the future.

Weaponization of IoCs

Itzik Kotler, ICIT Fellow and Co-Founder and CTO, SafeBreach, opines, "I think we should do more, not more of the same, but more on the reactive front of security which I think is a missed opportunity in this EO. With respect to sharing data, adopting new architecture, and monitoring - the real game-changer, in my opinion - will be weaponizing the IoCs that we know today to proactively assess whether emerging threats are applicable (i.e., detected & mitigated). There is a huge difference between buying/installing a given security control and making sure it's effective (and reasons why it may not be effective, can range from adversary tampering to IT changes that render it useless as a chokepoint). If we want to change this asymmetrical war with hackers, we first need to bring them to a position where their R&D costs will be so high it will not make financial sense to conduct. How? By continuously taking all the malicious knowledge out there (some publicly share, some privately share) and simulate it to test their security posture. By doing so and follow-up on the results, the companies will greatly reduce their chances of getting breached the same way." Jim Routh counters that given the breadth of the attack surface of the US, it behooves leaders to adjust federal cyber policy and practices to invest in proactive and protective solutions rather than offensive capabilities such as buying zero-day vulnerabilities.

Challenges Around Modernization and MFA Adoption

The Executive Order requires modernization planning and the adoption of multifactor authentication solutions where possible; however, Kevin Hansen, CTO, Federal Channels and Alliances, Micro Focus Government Solutions, suggests that modernizing some federal systems enough to support multifactor authentication (MFA) may be a prolonged process. He explains, "Much like the challenges agencies faced in delivering emergency support and services to citizens during the COVID pandemic, agencies have been hampered by technical limitations with these legacy applications. In the case of enabling MFA for mainframes, most of the mainframe interfaces users connect to do not have MFA support of any kind. In particular, those interfaces that still require a terminal emulator and older network protocols to connect to them (3270, VT, UTS, T27, telnet, INT1, FTP, SSH, etc. vs. a web browser/HTTPS) were never designed for MFA and have no common authentication standards support other than userIDs and passwords. Cutting to the chase, this means most of these green-screen applications are still using userID and password to login to mainframes – all across the government. A common "workaround" is to record a users' userID and password into an SSO script to automate the login after the user uses MFA to get onto the network. That's a convenient workaround for the user but unfortunately does not comply with HSPD-12 or the latest executive order, which requires a unique MFA challenge when accessing a different system (mainframe data). Of course, as the Executive Order states in Sec. 3 (d), '*Within 180 days of the date of this order, agencies shall adopt multifactor authentication and encryption for data at rest and in transit, to the maximum extent consistent with federal records laws and other applicable laws*.' So a successful network MFA should not grant access to all applications and data on the network – the applications and data require their own unique MFA challenge. Applying zero trust principles to this scenario further reinforces this requirement. The software tools necessary to solve these interface MFA challenges on the mainframes do exist but require a mandate and the explicit language in the Executive Order to shift agency priorities and resolve this once and for all.

Improving Public-Private Collaboration

The Executive Order strives to improve information sharing and oversight of federal contractors; however, it does not leverage the insights of public sector leaders to inform novel security strategies or combat emerging threats. Michael Aisenberg, ICIT Fellow and Chief Cyber Policy Counsel, MITRE, expounds, "The persistent shortcoming of DECADES of effort at addressing the panoply of cybersecurity risks facing the U.S. and global infrastructures is the failure of policy setting and funding government apparatus to fully appreciate the nature, construct and motivating elements of the private sector producers and users of ICT, and its growing infusion into every other critical infrastructure. Over and over again, the government, including the Biden Administration, in its important new EO, have failed to develop a construct that obligates bidirectional collaboration between the ICT industry and government and the other critical infrastructures. The failure to have a meeting of the minds about risk, trust, and

mutual obligations will continue to stand as a handicap to success in addressing the constantly evolving threats to ICT as deployed globally. Step one must be a process of deeply embedding government staff in C-suite roles in industry, and industry seniors in roles that expose them to the realities of government policymaking and execution."

The Executive order is predominantly focused on improving the cybersecurity of federal contractor solutions; however, in the future, it may be proactive to incentivize the private sector to increase collaborative threat intelligence efforts with the federal government. Stan Mierzwa, Director, Center for Cybersecurity, Kean University, explains, "The use of incentive programs in cybersecurity has been in existence for some time now. These programs allow for crowdsourcing the research, software bug detection, and vulnerabilities with a reward or incentive and are often referred to as Vulnerability Reward Programs [4]. Such incentivized programs may garner greater interest from both government agencies and the private sector, an increasingly important element in teamed or collaborative cybersecurity knowledge-sharing activities. A reference or example blueprint for this program can be gained from one announced and introduced several years back by the Pentagon [4]. The configuration of this effort provided ethical hackers with incentives to break into systems and report vulnerabilities for a reward [5]. One potential benefit of such a program is to drive community engagement to protect our critical infrastructures. At a minimum, consideration for such a reward program could be further researched to understand if it could add potential positive cybersecurity benefit, given the increasing, persistent, and more complicated attacks."

Internal Federal Software Supply Chain Risk Management (SCRM)

The Executive Order institutes greater governance on contractor solutions and mandates the adoption of security paradigms like zero trust and security by design; however, it is predominantly outward-facing. David Wray, ICIT Fellow and CTO, Micro Focus Government Solutions, explains, "I like the EO, but its impact all depends on the guidance that OMB produces for agencies and the changes they make to the FAR/DFAR in the next 3 to six months. The weakest link in the software development life cycle is the government agencies' custom code and applications, not commercial software vendors. The focus is on the vendor community and most likely will result in audits of vendors' software manufacturing process to ensure that a bill of materials is available, software is scanned for vulnerabilities, and secure practices such as zero-trust, threat modeling, and auditing are part of a vendors software production process. These are all valid asks; however, there was no mention of these requirements being mandated on the 10's of 1000's of custom applications in use today across government. Most of the critical software in government are mission support applications developed with open source, COTS/Tools, and custom code. It would be nice if agencies were required to scan code; but, there is no requirement across all agencies to do this today. There also is no requirement for a bill of materials or documentation on open source libraries, APIs,

etc. So, in my opinion, the focus of the EO on the commercial software vendor community is misguided. I believe it's sorely needed for open source producers, especially with libraries and add-ins used during the build process (IoC, for example). OMB could interpret these mandates as applicable to system integrators that support government software development efforts and prioritize open source and API/Binaries used during DevOps vs. COTS products. This would help close the gap; however, implementation would be challenging (scope changes on existing contracts). I would rather see the law codified that enforces code scanning, especially for opensource and binaries, or in some cases restricting the use of open source when there are known issues or poorly managed communities."

Integration of Cybersecurity Ethics Reinforcement

The Executive Order does not address federal cyber hygiene or potential insider threats. Increasing cyber hygiene efforts can help to "keep honest people honest" and reduce the likelihood of intentional or unintentional insider threats. Further, an ethics program can ensure that data is protected and used according to its intent upon collection. Mr. Mierzwa proffers that "The topic of ethics in computer science, information technology, engineering, and the sciences is not a new element. Students in many technical and non-technical programs are required to learn about the impact of ethical principles as they embark on careers in creating and building solutions to solve problems. The use of technology for bad actor activities is one of the harmful byproducts of cybersecurity knowledge. However, it is not just about bad actors; those who function in routine cybersecurity roles may come across situations when their best ethical judgment is required. In performing a quick search of the executive order for the word "ethics," no results were found. A suggestion to research or find ways to include cybersecurity ethics into the modules or sections of the executive order may be beneficial. At a minimum, a reinforcement of the topic to ensure that all involved in protecting our critical infrastructure assets are on the same page could be a good reminder. By laying a foundation of good ethics, there is the potential for better decisions when one is facing cybersecurity challenges [6].

Creation of a National Campaign

Mr. Mierzwa observes that the introduction of the Executive Order drew national attention and increased public discourse around federal cybersecurity, although members of the public may never delve into the details of the executive order. Worse, vendors and private sector organizations may not pay adequate attention to the reforms, recommendations, and frameworks that emerge from the directives issued by the EO. A public awareness campaign could be leveraged to increase awareness around the deliverables and incentivize public comment and participation. Though it may appear insignificant, lasting cybersecurity reform may depend on the public "buy-in" that results from increased attention and discourse.

ICIT Executive Director Joyce Hunter believes there is a need for a novel approach to public-private sector collaboration to facilitate information sharing and reduce operational, reputational, and financial risks. A public-private cyber intelligence and information exchange would enable more contextualized threat intel to allow organizations to better defend against advanced persistent threats. With its focus on commercial reporting of cyber incidents, the Executive Order begins to set the foundation for a new model; however, more needs to be done to ensure that collaboration, coordination, and communication do not end with only information sharing.

Conclusion

President Biden's Executive Order on Improving the Nation's Cybersecurity is an admirable effort to improve the cybersecurity and resiliency of federal agency systems, networks, assets, and solutions. The EO addresses many of the challenges jeopardizing federal systems, and it lays the foundation for further cybersecurity reforms. Some proactive topics to consider as federal cybersecurity is reformed include:

- How can the nation better utilize IoCs and proactively adapt to combat emerging threats?
- Are agencies' modernization and technology adoption challenges being addressed?
- What steps are being taken to improve Public-Private collaboration?
- Can agencies do more to secure internally developed and open-source solutions?
- Which programs are being developed to address national cyber-hygiene and ethics?
- Should more be done to socialize federal cybersecurity efforts to the public?

Finally, the administration should consider whether federal agencies have the workforce and resources necessary to meet the directives of the Executive Order or build upon its foundation. The EO is proactive and ambitious in its approach to cybersecurity reform, and that is commendable; however, it also contains 46 deadlines ranging from 14 days to one year. The timeframe is too narrow to identify, hire, and train new talent; especially if candidates must undergo background checks and clearance processes. Instead, agencies could consider retraining existing personnel in cyber-defense principles and best practices through accredited education programs offered by universities around the country. Many such programs are now offer asynchronous and remote instruction. While cybersecurity leadership is important, it is well-educated and trained practitioners in the trenches who will be executing the security controls. In cybersecurity, execution effectiveness is everything.

Sources

[1] "Executive Order on Improving the Nation's Cybersecurity | The White House", *The White House*, 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. [Accessed: 07- Jun- 2021].

[2] "FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks | The White House", *The White House*, 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/. [Accessed: 07- Jun- 2021].

[3] D. Maclean, "Executive Order on Improving the Nation’s Cybersecurity | DLT, a Tech Data company", *Dlt.com*, 2021. [Online]. Available: https://www.dlt.com/blog/2021/05/18/executive-order-improving-nation-s-cybersecurity. [Accessed: 07- Jun- 2021].

[4] C. Akemi T. and R. Chris, "Crowdsourced cybersecurity innovation: The case of the Pentagon’s vulnerability reward program", *Scholars.uow.edu.au*, 2018. [Online]. Available: https://scholars.uow.edu.au/display/publication128913. [Accessed: 07- Jun- 2021].

[5] T. Maillart, M. Zhao, J. Grossklags and J. Chuang, "Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs", *Journal of Cybersecurity*, vol. 3, no. 2, pp. 81-90, 2017. Available: 10.1093/cybsec/tyx008.

[6] M. Stan, R. S. and J. T., "Global Ethical and Societal Issues and Considerations with Cybersecurity in Digital Health: A rapid review.", *Northeast Data Sciences Institute.*, vol., 2021. [Accessed 7 June 2021].