

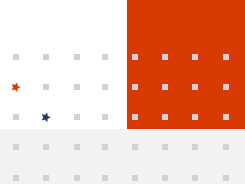


# Expanded cybersecurity policy for a more secure future

The [Cybersecurity EO](#) has the potential to accelerate profound advancements in security and resiliency across the federal enterprise. For both federal agencies and their technology providers, the EO outlines significant new steps to strengthen IT modernization, enhance software supply chain security, and improve incident response. Microsoft is committed to supporting implementation of the EO, helping others meet its requirements, and leveraging the opportunity it presents to foster cybersecurity improvements that impact our broader, interconnected ecosystem.

Microsoft has demonstrated our commitment to supporting implementation of the EO by engaging with agencies on software supply chain security best practices and standards, building upon our experience with

the [Security Development Lifecycle](#), and putting forward new thinking that reflects our focus on continuous improvement. We submitted position papers to [NIST's call for input](#), including on [source code testing](#), [security measures for use of critical software](#), and a proposed [Supply Chain Integrity Model](#). We also provided our [perspective](#) on minimum elements for a Software Bill of Materials, bringing together experts from our Cloud + Artificial Intelligence and Experiences and Devices engineering groups and from GitHub, where over 65 million users develop software. As implementation of the EO proceeds, we will remain committed to investing in public-private partnership to support federal agencies and our collective opportunity to advance security and resiliency.



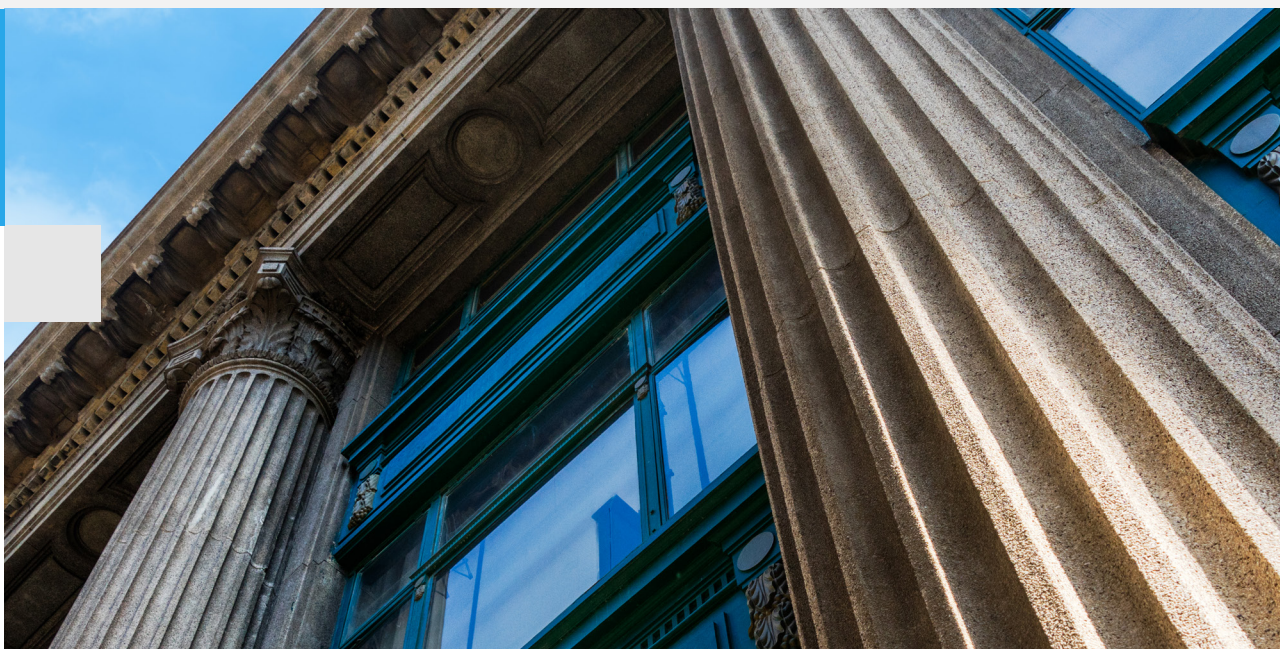
The [Executive Order on Improving the Nation's Cybersecurity \(Cybersecurity EO\)](#) is a welcome call-to-action to bolster the U.S. Government's resilience against cyberattacks. Over the last year, major attacks have shaken trust in the very technology the United States relies upon to remain innovative and secure. These attacks have also demonstrated the importance of continuously improving national and international cybersecurity strategies to deter and mitigate the impact of persistent cybersecurity threats. In his [testimony](#) to the U.S. Senate Select Committee on Intelligence following the attack on SolarWinds and its customers, Microsoft President Brad Smith recognized that:

---

*"...we all have important work to do to strengthen the nation's cybersecurity. We must be prepared for even more sophisticated and well-resourced foreign attacks in the future. We will need new measures that are grounded in leadership by the public sector and even more collaboration with the private sector."*

---

The dynamic and sophisticated threat environment, rapid pace of technology innovation, and scope of attack surface make holistically strengthening cybersecurity a complex endeavor. The Cybersecurity EO responds to this challenge by considering the lifecycle of technology adoption and management. It calls for modernizing federal government technology infrastructure, driving a consistent and high baseline for the security of both technology products and agency operations, and strengthening incident response and recovery. As new policies, guidance, and requirements are developed, Microsoft welcomes the opportunity to engage alongside public and private sector partners to foster common understanding and bring the breadth of our collective expertise to bear on these important efforts.





## Modernizing for security

The Cybersecurity EO recognizes that, if done well, modernization is security. It requires agencies to modernize their infrastructure, capabilities, and architectures to align with leading security practices. Specifically, it prompts agencies to move towards Zero Trust Architecture and refresh their digital transformation strategies, including through the deployment of cloud services. This strategy in the EO is further reinforced by the prioritization of cybersecurity investments as part of the [American Rescue Plan and the Technology Modernization Fund guidance](#).

Our experience managing Microsoft's environment and supporting customers has demonstrated the importance of embracing the cloud and adopting a Zero Trust mindset. As we closed our internal investigation of the SolarWinds attack in February, we [recognized](#) both practices as foundational to defending against future attacks. We underlined [how cloud services help](#) organizations prevent, detect, and respond to attacks and recommended that organizations [address gaps in protecting identities](#) as a first step in their Zero Trust journey. In 2019, the Government Accountability Office (GAO) also [reported](#) that nearly two thirds of surveyed agencies increased their use of cloud services from 2016-2019, realizing significant performance, security, and cost benefits.

Migration of legacy systems to cloud services could have cascading positive impacts on agency operations. [GAO has described critical U.S. Government legacy systems](#) that are insecure, have limited functionality, and are expensive to maintain. Cloud computing offers immediate benefits from a security perspective, including built-in architectures and services for [resiliency and reliability](#), [protection of sensitive data](#), and [proactive threat protection](#) – as well as greater functionality and reduced cost. As [GAO documented](#), in 2018, the cost to maintain a legacy U.S. Air Force system that provides operational support for aircraft was \$21.8 million (with annual costs expected to raise to \$35 million by 2020); after migrating the system to a cloud environment, the modernization “paid for itself” within five months, saving a projected \$356 million over a 10-year period, and enabled new functionality.

Migration to cloud services can be challenging, especially for legacy systems, but resources and services exist to support agency efforts. Wherever agencies are in their process of prioritizing workloads for cloud deployment, migrating data or other resources, or understanding how to maximize security investments while deploying cloud services, Microsoft is committed to partnership and sharing our experience. We offer [FastTrack](#), a service that helps customers plan for a successful cloud deployment, access personalized assistance as they migrate resources, and get the most value out of their IT investments. We've also published a [Cloud Adoption Framework](#) to provide agencies with mappings to key security concepts, frameworks, and standards as well as access to tools and templates they can leverage to establish baselines for strong cloud security and identity practices.





We've also compiled our top recommended Zero Trust tools and resources to help agencies assess their progress on Zero Trust, leverage step-by-step guidance on implementing Zero Trust principles, and reference technical guidance on deployment. Additionally, agencies already leveraging cloud service platforms like [Azure](#) or [Microsoft 365](#) can tap into the native security capabilities to quickly meet the Cybersecurity EO's directives to advance toward Zero Trust Architecture.

As agencies move more of their enterprise to cloud environments, the federal government must ensure a high minimum baseline for security of cloud offerings. The Federal Risk and Authorization Management Program ([FedRAMP](#)) is intended to accelerate agency adoption of cloud services that meet that high security bar, serving as a centralized hub for review of cloud security practices and awareness of cloud service provider and agency separate and shared security responsibilities.

Given agencies' efforts to rapidly modernize their environments, Microsoft welcomes the renewed emphasis and importance the Cybersecurity EO places on FedRAMP, including by calling for further modernization and automation of the program. The Cybersecurity EO also calls on the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA) to work closely with FedRAMP as they update and implement a new federal cloud security strategy, associated reference architectures, and cloud security principles. Additionally, recognizing agency-reported [challenges](#) with using FedRAMP, policymakers can update key directives, memos, and guidance underpinning the program as they chart a pathway to further equip and resource FedRAMP to keep pace with current and future demand for its services. Microsoft encourages policymakers to collaborate closely with cloud service providers that have years of experience [working with the FedRAMP program](#) and agency customers as they develop these mission-critical updates to the program as well as a supporting ecosystem of resources, including cloud security technical reference architectures.

# Driving a consistent and high baseline for security

Beyond calling for modernization, including through accelerated adoption of cloud services and a Zero Trust Architecture, the Cybersecurity EO focuses on specific areas of agency operations and technology products where there's a need for a consistent and high baseline for security.

For agency operations, these practices help with prioritization of steps to advance toward a Zero Trust Architecture. To Microsoft, [a Zero Trust mindset reflects three principles](#):

- Verify explicitly, always authenticating and authorizing based on all available data points;
- Use least privileged access, including through Just-in-Time and Just-Enough-Access policies; and
- Assume breach, segmenting and minimizing blast radius, including by verifying end-to-end encryption and using analytics to get visibility, drive threat detection, and improve defenses.

The Cybersecurity EO's specific requirements for agency security practices map to Microsoft's three principles and focus on particularly impactful foundational steps to their implementation. We're encouraged by the Cybersecurity EO's focus on use of multi-factor authentication (MFA), a key practice for verifying explicitly, and encryption for data at rest and in transit, a key practice for assuming breach. Microsoft's products encrypt data at rest and in transit, including [Azure](#) and [Microsoft 365](#) (see further context on [Exchange Online](#), [OneDrive](#) and [SharePoint](#), and [Teams](#) in particular as well as [technical reference details](#)), and enable use of MFA (including through [Azure Active Directory](#) and in [Microsoft 365](#)). Adoption of these practices will significantly improve risk management posture across the federal government; the [Microsoft Digital Defense Report](#) highlights the impacts of MFA in particular:

*"...more than 99% of password spray attacks use legacy authentication protocols, and more than 97% of credential stuffing attacks use legacy authentication. Given the frequency of passwords being guessed, phished, stolen with malware, or reused, it's critical for people to pair passwords with some form of strong credential. Therefore, disabling legacy authentication and enabling MFA is a critical call to action."*




The importance of MFA and encryption is also underlined in the [National Institute of Standards and Technology \(NIST\) security measures for agency use of EO-critical software](#) – along with other practices that are foundational to verifying explicitly, using least privileged access, and assuming breach. For example, NIST requires that agencies uniquely identify and authenticate each service attempting to access EO-critical software, follow privileged access management principles for network-based administration, employ boundary protection techniques (e.g., network segmentation and isolation), and continuously monitoring the security of EO-critical software.

NIST's security measures for agency use of EO-critical software also require practices to ensure that software is configured and maintained over time. Agencies must identify and implement proper hardened security configurations for EO-critical software as well as mitigate known vulnerabilities, including by patching and ensuring software is upgraded to a supported version.

Agencies also need to partner with software providers and operators that meet or exceed a high baseline for security, and the Cybersecurity EO outlines numerous requirements to ensure that federal software incorporates supply chain security best practices. Microsoft recognizes the importance of improving the security and integrity of the software supply chain and supports the Cybersecurity EO's focus on this area. As Brad Smith [shared](#) in February:

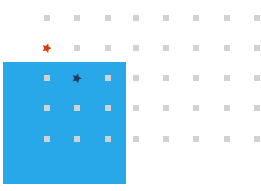
*"The public sector at all levels of government should strengthen the protection of their software, including through secure development practices, better software maintenance and vulnerability management, and integrity controls that apply throughout the software development, testing, and delivery processes."*

Fortunately, the federal government and private industry have for years partnered on software supply chain risk management. Microsoft has long invested in developing best practices for [secure software development](#), [source code testing](#), and [vulnerability disclosure and management programs](#). We've also contributed to efforts to define industry-wide practices and consensus standards on secure software development and vulnerability disclosure and management, including through [SAFECode](#), [ISO](#), and [NIST](#).



Along with GitHub, Microsoft has also contributed to efforts to develop best practices and specifications to define use cases for and support the delivery of a software bill of materials (SBOM). SBOMs identify what software is composed of and allow software providers to associate information with components. Efforts to define [“minimum elements” of an SBOM](#) explain what information should be associated for near-term use cases; however, over time, additional information could be attached to and conveyed through SBOMs as use cases that could take advantage of that information are identified. For example, whether a software component has gone through an audit could potentially be conveyed.

[Microsoft and GitHub support delivering SBOMs](#) to enable vulnerability analysis and integrity checks, and we’re committed to leveraging SBOMs as part of a broader evidence store that would verify end-to-end supply chain integrity. Microsoft has worked on internal formats to convey SBOM information for our own internal security risk management efforts, and we plan to use the Software Package Data Exchange (SPDX) – specifically, [SPDX 2.2](#) in the near term – as a preferred format to deliver SBOM information to customers. GitHub also makes available [dependency graph](#), which identifies a project’s dependencies and [supports several package manager and manifest formats](#). To help protect open source projects, dependency graph is on by default for public repositories. GitHub’s knowledge of a project’s dependencies, combined with its open and curated advisory database, [can automatically detect, alert, and remediate vulnerable dependencies](#). Both Microsoft and GitHub are also actively participating in the development of SPDX, including ongoing efforts to define SPDX 3.0, which is on track to support a broader set of SBOM use cases.



We also recognize that efforts to develop software supply chain security requirements, including for SBOM and other areas as required by the Cybersecurity EO, are ongoing, and we welcome opportunities to continue to engage with NIST, the National Telecommunications and Information Administration (NTIA), and other government partners as those efforts to deliver on EO taskings proceed. Microsoft has valued the input opportunities that NIST and NTIA have already facilitated; we’ve submitted position papers to [NIST’s call for input](#), including on a proposed [Supply Chain Integrity Model](#), and shared our [perspective](#) on minimum SBOM elements with NTIA.

However, much work remains to be done, including on the specific software supply chain security requirements resulting from the Cybersecurity EO and on ecosystem readiness for broad and rapid adoption of SBOMs. For example, consideration of [BOM use cases and delivery models for cloud services requires attention and public-private partnership](#). Cloud services have unique requirements in how they are described, how integrity is verified, and how vulnerabilities are published and shared, and the delivery of cloud services is fundamentally different than that of software run and maintained by users in their own environment. Efforts to address outstanding issues and provide greater clarity, including through forums like a multistakeholder working group, would facilitate implementation of the Cybersecurity EO. Iterative policy development and implementation, reflecting shared understanding and direction among government policymakers and industry operators and experts, is key to effectively addressing complex cybersecurity challenges facing our nation.



Getting it right is especially important given the opportunity the Cybersecurity EO presents to cascade security best practices across our broader, interconnected ecosystem. The EO calls for consumer Internet of Things (IoT) and software labeling pilots, presenting an opportunity to extend elements of baselines defined for the federal environment to other technology users. Recognizing limitations given that labels reflect a point-in-time evaluation, Microsoft supports the government's efforts to focus on improving transparency into security practices for consumer software and IoT products and welcomes

the opportunity to contribute to the development of criteria and pilots. We also recognize the applicability of existing efforts, such as implementation of the IoT Cybersecurity Improvement Act of 2020, and best practices, such as [NISTIR 8259](#), [ETSI EN 303 645](#), and [ISO/IEC 27402](#). Consistency with internationally recognized standards developed through consensus-based processes brings focus to widely recognized best practices and allows organizations that operate around the world to create and maintain interoperable approaches to cybersecurity risk management.

## Strengthening incident detection, response, and recovery

Modernizing systems and infrastructure and implementing a consistent and high baseline for the security of both technology products and agency operations will significantly improve the government's cybersecurity posture. However, the threats we face will continue to evolve, and organizations must continue to respond to and recover from incidents. A [Zero Trust mindset](#) requires organizations to assume breach, and strengthening cybersecurity incident response across the public and private sectors is a theme throughout the Cybersecurity EO. It appropriately focuses on ensuring technologies and process are in place to detect anomalies, conduct investigations, and remediate issues.

A first step is ensuring the right technology capabilities are in place to improve visibility and drive automated detection and response. Through modernization and use of cloud services, agencies can benefit from threat intelligence and powerful AI; [Microsoft's platforms and services assess over eight trillion security signals](#)

[every day](#) and surface and correlate security alerts that could represent a larger issue (or remediate issues on demand with our own threat experts). In addition, deploying consistent approaches to endpoint detection and response (EDR) will enable government-wide threat hunting, and maintaining sufficient logs will provide critical data for investigations and remediation efforts. To help our federal partners fully leverage the benefits of maintaining logs, Microsoft is [offering](#) all U.S. federal government customers who use our Government Cloud a one-year free trial of [Advanced Audit](#).

As agencies acquire and deploy these capabilities, Microsoft encourages agencies' CIOs, CISOs, and other senior leadership to enhance visibility into their current assets and to ensure that EDR, MFA, encryption, and other security solutions work across multiple devices and environments. If executed with this goal in mind, agencies will develop clarity over their threat surface and enable enhanced threat hunting across their networks and systems.





Microsoft also supports the development of processes to enable the government and industry to more effectively plan and utilize lessons learned for continuously improved coordination, response, and recovery. We're encouraged by the establishment of the Cyber Safety Review Board and concur on the need for government and industry to work closely together to understand and learn from significant incidents that impact both the public and private sectors. Standardizing incident response and vulnerability management playbooks is also an important step. Given the role the private sector often plays in partnering with agencies on incident response and recovery, Microsoft encourages policymakers to welcome private sector input as the playbooks are developed, leveraging a process akin to that managed in 2016 for the development of the National Cyber Incident Response Plan.

Several sections of the Cybersecurity EO set in motion processes for requiring companies to share cybersecurity incident information with their federal customers and with CISA. Well-defined and coordinated incident reporting strengthens the collective defense and response of both the federal government and private companies. Microsoft President Brad Smith underlined the need for incident reporting obligations in his testimony before the Senate:

Microsoft encourages policymakers to consider several key areas when requiring incident reporting information. Specifically, the government should ensure that appropriate thresholds for reporting are well defined, the types of information that need to be reported are well understood, the risks associated with short reporting timelines are recognized, and there is a single government point of contact for reporting across federal civilian agencies. Additionally, given the patchwork of obligations that already exist, Microsoft encourages policymakers to minimize duplicative reporting where possible.

Sharing incident response information back with private sector first responders can also further accelerate incident response and recovery. As Microsoft President Brad Smith further highlighted to the Senate:

*"Disclosure should not be limited to just the private sector. In exchange for imposing [an incident reporting obligation], the government should also commit to faster and more comprehensive sharing of relevant information with the relevant security community."*

*"Transparency in incident response is extremely challenging...But transparency also enables more effective incident response...We need to replace [the silence we've seen after recent attacks] with a clear, consistent obligation for private sector organizations to disclose when they're impacted by confirmed significant incidents."*

Microsoft believes key stakeholders across the public and private sectors must work together and invest in our shared responsibility to improve cybersecurity. We have a common goal of protecting government operations and the broader ecosystem and facilitating recovery when incidents occur. Continued collaboration and regular stakeholder engagement will help drive effective implementation around response and recovery efforts as well as the many other objectives outlined in the Cybersecurity EO. We stand ready to support our public sector partners as they achieve the EO's goals and their core missions.