“The draft United States executive order on cybersecurity”

The Accenture Cybersecurity Forum (ACF) convened a special session titled, “The draft United States executive order on cybersecurity,” on April 22, 2021.

An executive order (EO), spurred by the SolarWinds cyberattack, is expected to be issued by the federal government in the coming weeks. The EO is meant to improve the government’s ability to detect, coordinate, respond to and investigate cybersecurity incidents while also raising costs for attackers and improving software supply chain security.

During this special session we reviewed our current understanding of the draft EO at a high level to gain members’ initial insights and reactions. We also discussed members’ critical priorities—both for enterprises and for government—that could emerge from this initiative.

Our speakers included Accenture Security subject-matter experts, enterprise CISOs and board members.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

Overview:
While most of the EO is intended to improve federal government cyber resilience it will have both a direct and indirect impact on the private sector by creating requirements and market incentives for more secure IT and OT software, including cloud, hybrid and on-prem.

Sec. 1: Improving government coordination on significant cybersecurity incidents:
The Deputy National Security Advisor for Cyber and Emerging Technologies will be responsible for overall coordination and integration of cyber policy and strategy. PPD 41 will be amended to reflect this. The EO will call for the establishment the Cyber Unified Coordination Group. PPD 41 will also be amended to reflect that FBI and the National Cyber Investigative Joint Task Force are lead federal agencies for threat response activity. CISA will lead for threat response; ODNI will lead for intelligence support and related activities.

Sec. 2: Standardizing the federal government playbook for responding to cyber incidents:
Within 120 days, DHS Secretary and OMB, plus federal CIOs, the Federal CISO Council, Attorney General, NIST, and NSA shall develop a standard playbook. It will be used in planning and

conducting cyber incident response on federal systems, including national security systems. The OMB director shall issue guidance to mandate use of the playbook. The CISA director will review the playbook annually, provide OMB updates and then OMB will use this to provide agencies as annual FISMA guidance.

Sec. 3: Improving detection of cybersecurity incidents on federal government networks:

a) Federal/civilian Endpoint Detection and Response (EDR) Initiative—Within 30 days, the CISA director shall provide OMB recommendations on implementation approaches to a centralized EDR initiative. Within 90 days of receipt, OMB shall issue policy requiring government-wide EDR approaches, supporting centralized CISA managed cyber hunt, detection and response.
b) Adequate resourcing of above will be overseen by OMB
c) Within 45 days, departments and agencies shall establish MOUs with CISA for CDM to ensure object level data is available and accessible to CISA.
d) Within 45 days of EO, CISA shall provide a report on threat hunt activities on federal networks as authorized by NDAA. Thereafter, quarterly reports must be provided.

Sec. 4: Improving federal government investigative and remediation capabilities:

a) Within 14 days of EO, DHS shall provide OMB recommendations on requirements for logging events and retaining other relevant data within each department/agency network.
b) Within 90 days of receiving the recommendations above, OMB shall issue policy establishing requirements for logging, log retention, log management and centralization of top-level department and agency security operations centers.
c) OMB shall work to make sure above is resourced.

Sec. 5: Removing barriers to threat information sharing within the federal government:

a) Within 60 days, the OMB director shall review Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation (DFAR) contract language requirements and provide updated contract language to the FAR council.
b) Contracts shall contain no barriers to
    a. Data that service providers collect related to event prevention, detection and response; sharing of this data; collaborate with CISA and FBI investigations; any addition steps necessary.
c) Within 120 days, FAR council shall review contract language and publish it for public comment.
d) Within 120 days, OMB and DHS shall implement actions that ensure that existing contracts allow data sharing consistent with FAR Council language.
e) Software and SaaS providers that enter into federal contracts must promptly report to federal customers and CISA when a cybersecurity incident or breach is discovered, involving a software product or service provided to the federal government or a support system to a software product or service provided to the federal government. CISA will centrally collect and manage this information.
    a. Within 45 days, DHS will recommend to the FAR Council contract language to implement this. Within 90 days of receipt, the FAR Council shall publish for public comment.
    b. Within 90 days of EO, DHS, the Attorney General and ODNI will develop procedures for cyber incident reports to be promptly filed and appropriately shared.

c. Within 60 days, DHS will identify and recommend cybersecurity requirements that are common across federal agencies that could be standardized and recommend contract language to the FAR Council.
d. Within 180 days, DHS and Department of Commerce shall provide a report to the President assessing additional options to reduce cybersecurity risk to federal agencies from potentially insecure commercial IT services.

Sec. 6: Modernizing federal government cybersecurity through increased adoption of best practices, increase adoption of zero trust, and accelerated move to SaaS, IaaS and PaaS:

a) Within 60 days, each federal agency will update agency plans to prioritize resources for the adoption and usage of cloud technology; develop a plan to migrate toward a zero trust model.
b) DHS and GSA will modernize FedRAMP to facilitate this.
    a. Within 90 days, DHS shall develop a federal cloud security strategy that moves the federal government closer to a true centralized enterprise model that incorporates zero trust.
    b. Within 90 days, DHS shall develop and issue a federal/civilian-wide cloud security technical reference architecture.
    c. Within 60 days, CISA director will develop a federal cloud service governance framework.
    d. Within 90 days, agency heads will report to OMB and CISA with an evaluation of the types and sensitivity of the agency's unclassified data.
    e. Within 30 days, agency heads will report on implementation of multifactor authentication and encryption for data at rest and in-transit. Reports subsequently required every 90 days until full adoption.
    f. Within 90 days, CISA and FedRAMP shall establish a framework to coordinate and collaborate on cybersecurity and incident response activity related to cloud technology.

Sec. 7: Establishing a cybersecurity incident review board:

DHS and AG will establish the cybersecurity incident review board. The board will review and assess threat activity, vulnerability, mitigation activities and federal government response actions.

Sec. 8: Enhancing software supply chain security:

a) Within 30 days, Sec. of Commerce shall initiate a dialogue with private sector, academia, others to identify standards, best practices and other guideline to assist software developers. Within 180 days, NIST shall publish preliminary guidance. Within 360 days, NIST shall publish additional guidance.
b) Within 60 days, Sec. of Commerce will promulgate an initial list of secure software development lifecycle standards acceptable for the development of software for purchase by the US Government. Consistent with the above, all commercial suppliers of software available for purchase by the federal government share comply with, and attest to:
    a. Development environment: SDL processes; security of software development environments; generating and when requested providing artifacts that demonstrate conformance; maintaining accurate and up-to-date controls for internal and third-party software components and tools present in their development process; participating in a vulnerability disclosure program; publishing a SBOM for each product.

    b. Software: Ensure and attest to the integrity and provenance of the code, prior to product, version or update release; employ automated tools or comparable process that checks for own and potential vulnerabilities, conducted regularly or at least prior to product, version or update release; providing artifacts of the aforementioned to government.
    c. Open source software: developers must attest to the integrity of the open source they use
c) Identify critical software
    a. Within 45 days, Sec. of Commerce will specify criteria for designating "critical software."
    b. Within 75 days, CISA shall identify and make available to government entities what meets the critical software criteria.
    c. Within 60 days, Sec. of Commerce shall promulgate guidelines outlining security measures to be applied to critical software. These guidelines must be implemented within 120 days of this EO, or 60 days after NIST promulgates guidelines.
d) Government side software procurement
    a. Within 120 days, critical software must be developed in conformance with NIST standards for federal buyers to buy it.
    b. Within 180 days, only software that developed in conformance with NIST standards shall be eligible for federal procurement.
    c. Within 180 days, GSA will take critical software off of the federal supply schedule if it doesn't comply with development requirements. Noncritical software comes off the list within a year.
    d. Within 180 days, DHS will provide the FAR Council with language requiring commercial software suppliers to conform with requirements above.
e) Legacy software
    a. Critical software must meet requirements or have a plan to do so. Non-critical software must do the same.
f) Software Bill of Materials
    a. Within 60 days, Sec. of Commerce shall promulgate minimum elements for products eligible for federal procurement. Within 30 days, a plan will be issued for software bill of materials for "critical software."
g) Within 60 days, Sec. of Commerce will issue minimal requirements for pen testing and auditing, to include automated tools, for source code for software.
h) Pilot programs
    a. IoT: Within 180 days, FTC Chair will initiate a program including ratings and labeling.
    b. Software assurance: Within 210 days, FTC chair will initiate a program including ratings and labeling.

CISO perspectives and priorities:

ACF members and subject-matter experts expressed a variety of questions and concerns about the forthcoming cybersecurity EO.

- This EO is seen as a significant incremental change in cybersecurity requirements. CISOs can help boards of directors and leadership teams prepare for possible implications including breach disclosure requirements, potential litigation, shareholder concerns, technology

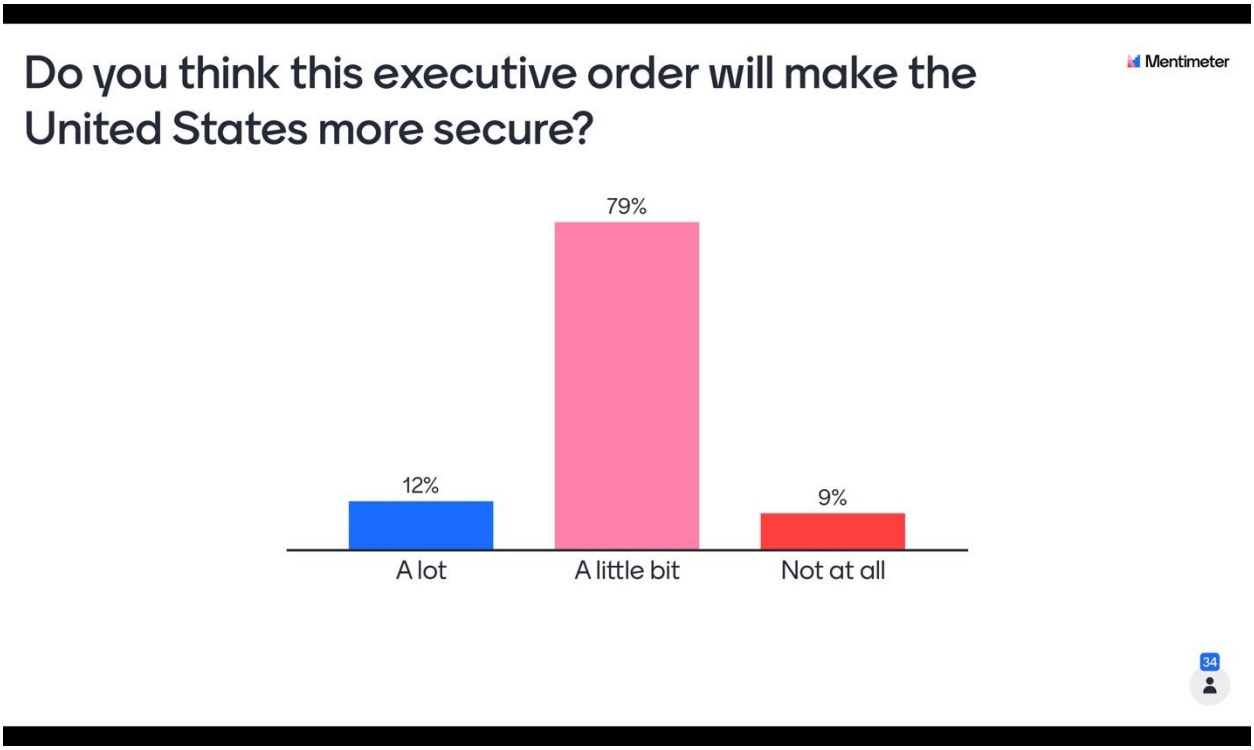
sourcing and the opportunity to build trusted cybersecurity to enhance enterprise reputation and as a competitive advantage.

- A board member said uncertainty about the details of the EO underscores the importance of have a cyber risk committee of the board. “Sometimes there is initial trepidation, but in every case I’ve been involved in, the CISO and the cyber team eventually see the value.” He added that the board’s concerns should now extend beyond shareholder demands, disclosure, and litigation risk to raising the bar on the products and services the enterprise buys. “Ask your vendors about their security capabilities,” he said. “Do they have a CISO? A secure coding program? Are they following the same practices outlined in the EO?”
- Participating in industry working groups, task forces and NIST can help CISOs be aware of proposed changes sooner, allowing for adaptive response and early preparation as a competitive advantage. One Forum member said: “The government will need a lot of help to make sure that requirements are effective and practical.”
- Because the EO is an incremental step, many questions will need to be addressed, such as which incidents warrant reporting and liability protection. CISOs foresee this potentially leading to increased litigation and wonder what kind of liability protections could be had with an increase in sharing incident response information with government. A Forum member and lawyer said: “We can expect to see more reporting about incidents. We’re going to hear a lot more about things that used to be swept under the rug. And with that increase, there will be more litigation, even if we don’t know exactly how that will play out. The EO cannot provide liability protection; that requires legislation. But the Cybersecurity Information Sharing Act may still apply, and that does have certain liability protections.”
- Defining what constitutes an “incident” is a particular CISO concern. This is an area where CISO input can help the government develop standards that are effective and practical. A subject-matter expert said that setting standards by industry may be the most effective approach for influencing CISA.
- EO requirements will likely become de facto standards. A CISO pointed to a positive “trickle-down implications” of the federal government putting new cybersecurity demands on software providers. Other members noted that smaller firms may struggle to meet new requirements, resulting in a bifurcated marketplace. While some companies may be more sophisticated than the federal government in terms of software development, CISOs agreed that if a “low bar” regulation is set, higher standards should be maintained.
- Several Forum participants noted that having big companies replicate the eventual software requirements for the federal sector would be a huge win. A board member said that smart boards will be familiar with the EO and want enterprises to follow those requirements.
- For government suppliers the EO presents a significant transformation opportunity to further mature or adopt cloud, zero trust, MFA everywhere, incident tracking and reporting and other practices.
- CISOs of companies (or perhaps all) should reassess their own ability to meet new federal standards. First to move may be able to secure more contracts.
- In enhancing software supply chain security, a subject-matter expert said: “The government intends to ask for evidence of activity (e.g. testing metrics or results) so it will be more than just getting vendors to say ‘we did X.’” He added: “Once there is a standard across the whole federal government, I suspect the government will also implement a process to qualify third-party auditors whose results will have to be accepted by any government agency.”

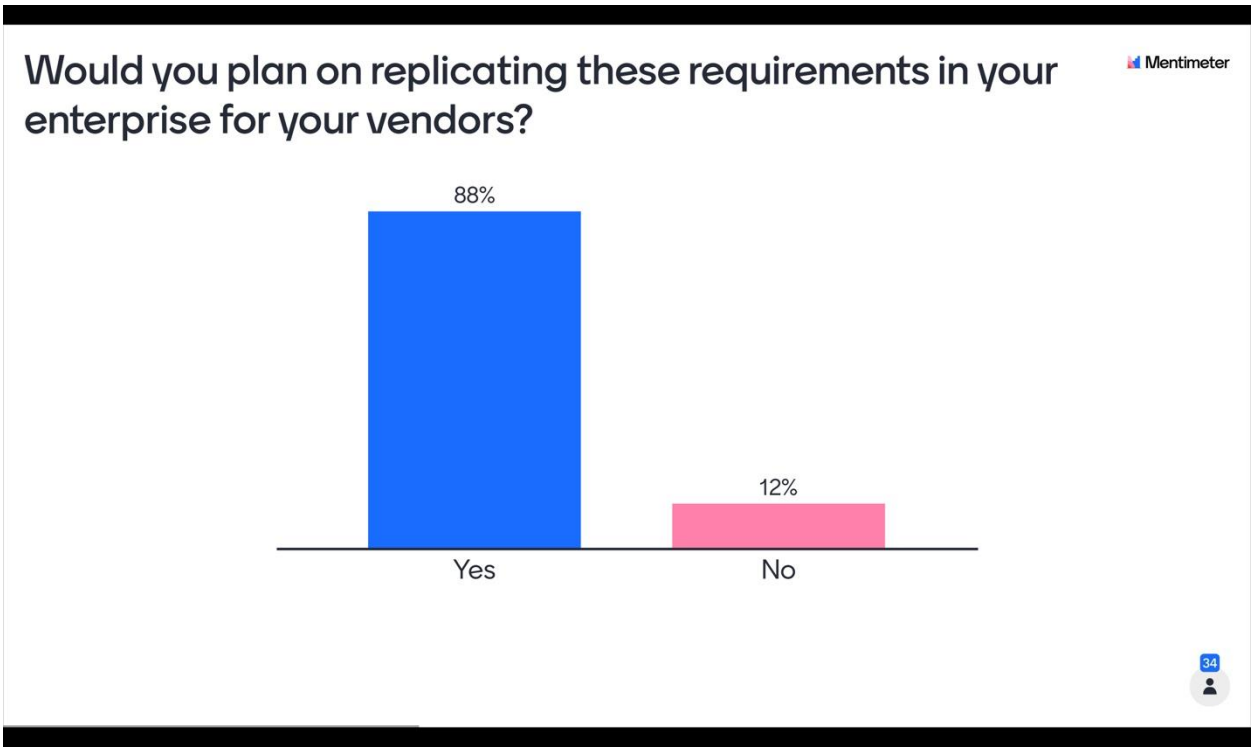
- A CISO suggested a "trusted" service for doing third-party assessment. “This would allow companies to leverage a service instead of trying to replicate all of the requirements themselves at a much higher cost. This could be a higher quality and defined assessment that any size company could leverage and be confident that a third party is doing what is right.”
- Global CISOs will need to monitor the potential impact of data localization requirements, emerging standards outside the U.S. and possibly conflicting breach disclosure requirements. “In the short term, the EO will affect any enterprise that has a contract with the federal government,” said a subject-matter expert. “But longer term, this might contribute to the fragmentation of the internet.”

Polling results:

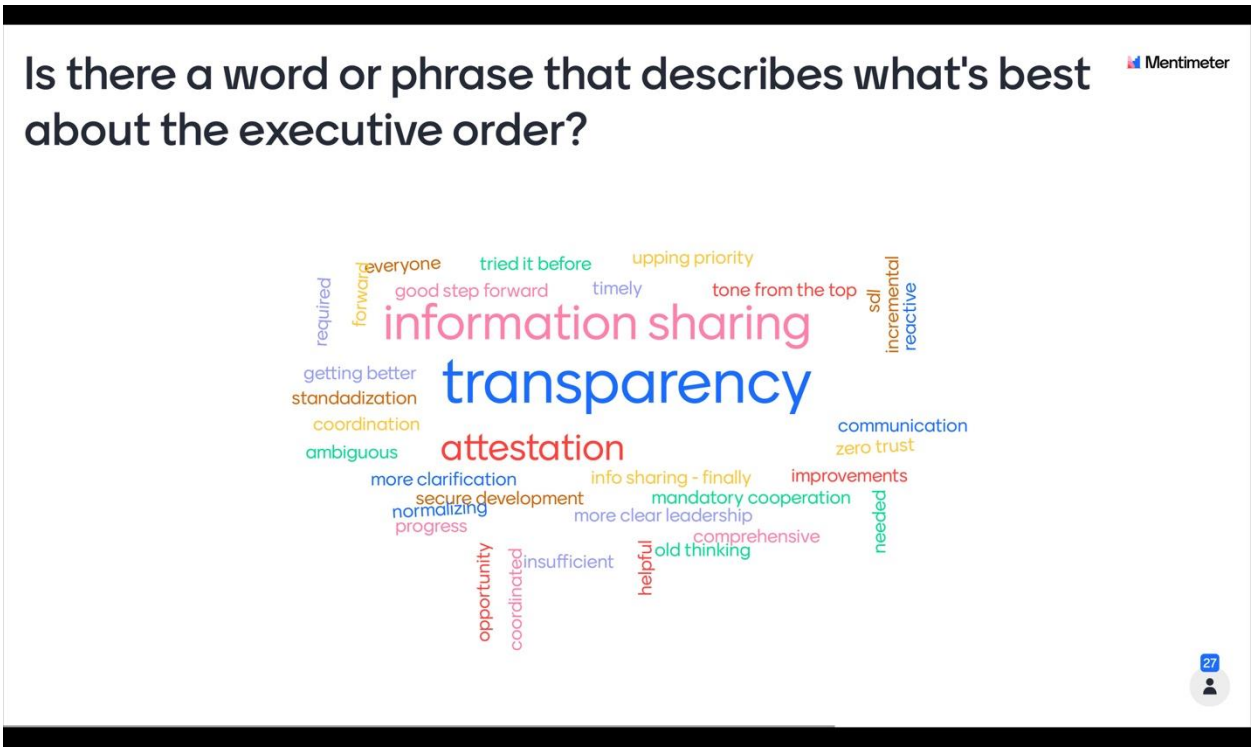
Forum members were surveyed for their opinions about the impact of the EO.



Almost 80% of surveyed members thought that the EO would make the US “a little bit” more secure.



It appears that the EO SDLC requirements may become a de facto standard: 88% of Forum members surveyed said that they plan to replicate these requirements for their enterprise vendors with 12% saying “no.” It is worth noting that at least one and probably all of the respondents who said “no” were from companies based outside the US.



The terms “transparency” and “information sharing” were expressed when Forum members were asked for a word or phrase that describes what they think is best about the EO.

Conclusion

The United States draft executive order on cybersecurity represents significant change—and opportunity—for both federal contractors and commercial enterprises. For example, by removing contractual barriers that inhibited the ability of federal agencies to share threat intelligence, the federal government is promoting greater transparency and data sharing. This could normalize information-sharing at both the government and commercial levels, contributing to stronger cyber defenses, but also increasing the risk of litigation.

In defining secure software development lifecycle standards for software purchased by the US government, the EO will likely set de facto standards that raise the bar for software supply chain security. Software vendors should expect CISOs to ask about secure coding practices and EO compliance. Software companies that quickly comply with new standards may have a competitive advantage while those slow to respond may be left behind.

CISOs, the C-suite and boards of directors are encouraged to guide their enterprises in quickly getting ahead of the curve. Engage with the federal government and standards authorities to drive practices and requirements that are effective and practical. Weigh the advantages of becoming an early adopter to create competitive advantage and address the unintentional consequences of litigation, greater disclosure requirements and playbook revisions. By looking at the EO through the lenses of people, processes and technology, CISOs will use this EO as an opportunity to increase their cyber resilience.

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 537,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.