HOW IS SAS RESPONDING TO THE CYBERSECURITY EXECUTIVE ORDER 14028?

Abstract

With this Cybersecurity Executive Order, SAS remains steadfastly committed to delivering and maintaining secure analytics solutions.

SAS recognizes that security is a critical aspect of the work that we do. We welcome the additional oversight and emphasis on cybersecurity that this executive order (EO) brings to the industry. SAS has always sought to responsibly avoid and mitigate security risks by managing vulnerabilities identified in our software and its integrated third-party components.

We continue to prioritize cybersecurity

Customers have trusted SAS for more than four decades to handle their mission-critical information. SAS works diligently to maintain that trust. We continuously monitor emerging technologies and industry best practices for strengthening cybersecurity and we work to incorporate them into each phase of our secure Software Development Lifecycle (SDL). Processes include:

- Leveraging industry-leading application security tools to perform:
    - Software Composition Analysis (SCA)
    - Static Analysis (SAST)
    - Dynamic Analysis (DAST)
    - Penetration Testing
    - Secure Architectural Design
- Monitoring the quality of our code used in our products as it moves from development to build to release environments to ensure it follows our software security policy before and after release.
- Employing advanced threat modeling techniques during design and operations phases to continuously analyze and improve the resiliency of our software against today's emerging cybersecurity threats.

- Documenting our commitment to security through the SAS Software Security Framework and Quality Imperative.
- Maintaining compliance and, where applicable, attaining certifications that offer independent validation of our adherence to best practices, such as ISO 27001, SOC2, and FedRAMP (current certification status available on the FedRAMP Marketplace).
- Maintaining membership in the Forum of Incident Response and Security Teams (FIRST) and participating in other industry security organizations.

Upon the May 12, 2021 EO release, SAS immediately formed a team to analyze the requirements, reassess our existing security initiatives, and develop an implementation plan. Efforts underway include:

- Initiatives to build greater levels of security transparency with our customers, including:
    - documentation as security
    - an evolving SDL institutionalized with product development
    - regular Building Security in Maturity Model (BSIMM) reviews and assessments
    - modeled and measured "secure by design," "secure by default," and "secure in deployment" in product code
- Ensuring that investments and resources align with the EO security objectives.
- Developing internal security talent through the creation of a product security lead (PSL) program. Our PSLs lead the strategic implementation of security initiatives for their divisions and provide education and guidance to enable the design, development, and deployment of secure software.
- Hiring a dedicated open source program manager to ensure we effectively document, test, and communicate the contents of our applications in order to comply with the EO and future agency actions. For example, generating the software bill of materials (SBOM).
- Enhancing our application security education efforts using industry and subject matter experts to create learning modules so that all product team members are well-prepared for increased security requirements for design, coding, and testing.
- Closely monitoring agency actions and guidance linked to the EO and following developments at NIST, NTIA, and OMB.

Our action plan will evolve as the federal government issues further guidance. We will update this web page accordingly. Please note that SAS does not discuss proprietary security information publicly. For more information, you may contact SAS Technical Support.

Background

In response to a series of crippling cyberattacks impacting various businesses, government agencies, utilities, and hospitals, President Biden signed an extensive Executive Order (E.O. 14028) on May 12, 2021 to acknowledge that the U.S. will continue to face unrelenting and increasingly severe cyber threats in the near future.

This Executive Order (EO) requires the creation of, and adherence to, new software security standards and best practices. It is primarily directed at federal departments and agencies and federal contractors. It is, however, implementing standards that will likely have a much broader impact across critical infrastructure sectors and related technology suppliers, including SAS.

The EO describes at a high level what the federal government wants to accomplish: enhancing software supply chain security. The specific standards and requirements that technology suppliers need to meet will be described in subsequent guidance and guidelines.

More Information

- Software Security Framework: www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/sas-software-security-framework-107607.pdf
- The Quality Imperative: www.sas.com/qualitypaper
- Security Assurance: www.sas.com/security-assurance
- SAS Trust Center: www.sas.com/trust
- SAS Technical Support: www.sas.com/support
- Corporate Social Responsibility: www.sas.com/csr