

NIST Publishes Draft Security Criteria for Consumer Software

December 1, 2021 Editorial Team

Compliance, Consumer Software, Cybersecurity, Data Security, Federal Trade Commission (FTC), NIST, Technology

0 Comments

Consumer software providers will soon have the option to label their software as compliant with National Institute of Standards and Technology (NIST) standards for software security. On November 1, 2021, NIST published its initial draft of this standard in a white paper titled "DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling" (the White Paper). The White Paper defines the security-related information that would have to be disclosed on the label and the specific security practices a software provider would have to follow. It was developed in coordination with the Federal Trade Commission (FTC) and will likely inform future FTC guidance and enforcement activity. NIST has requested public comments on the White Paper by December 16, 2021. The final version is expected to be published by February 6, 2022.

IN DEPTH

President Joe Biden's May 12, 2021, Executive Order (EO) 14028 directs NIST to initiate pilot programs for cybersecurity labeling "to educate the public on the security capabilities of Internet of things (IoT) devices and software development practices." Under the EO, NIST, in coordination with the FTC and other agencies, "shall identify secure software development practices or criteria for a consumer software labeling program." The criteria shall "reflect a baseline level of secure practices" as well as "increasingly comprehensive levels of testing and assessment that a product may have undergone."

The White Paper addresses the need to develop appropriate cybersecurity criteria for consumer software, which means software primarily used for personal, family or household purposes. It is intended to inform "the development and use of a label for consumer software," which would "improve consumers' awareness, information, and ability to make purchasing decisions while taking cybersecurity considerations into account." It is not intended to "describe how a cybersecurity label should be explicitly represented" or "detail how a labeling program should be owned or operated."

The White Paper has three primary elements: (i) it defines baseline technical criteria for the label; (ii) it details a proposed approach for conformity assessment; and (iii) it describes criteria for the labelling approach. It also enumerates specific issues on which NIST requests comment.

BASELINE TECHNICAL CRITERIA

The White Paper defines a series of outcome-based attestations (*i.e.*, claims) that software providers would make about their product on the NIST label. It also provides criteria for satisfying each attestation.

To meet the baseline technical criteria, software providers will need to implement the following practices:

- Follow the NIST Secure Software Development Framework (SSDF).
- Provide a mechanism for reporting vulnerabilities.
- Provide support at least until the published end-of-support date.
- Remediate all known vulnerabilities before the label date.
- Cryptographically sign the software and any updates.
- If user authentication is required, implement multifactor authentication or participate in an identity federation ecosystem that supports multifactor authentication.
- Remove passwords, encryption keys or other secrets from source code (*i.e.*, no hard-coded secrets).
- Follow NIST cryptographic standards for all encryption.

Search



Recent Posts

- [NIST Publishes Draft Security Criteria for Consumer Software](#)
- [Interest Groups Exert Influence as Support Grows for Federal Privacy Law](#)
- [CNIL Publishes White Paper on Digital Payments and Data Privacy](#)
- [FTC Report Reveals ISP Data Privacy Failures](#)
- [How to Manage the CIO-CMO Relationship](#)

AFFILIATE MEMBER



Recent Comments

- Justin on [CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS PROPOSED TEXT OF REGULATIONS](#)
- Joy Intriago on [Chief Compliance Officers Need to Know Cybersecurity](#)

AFFILIATE MEMBER



Categories

- [Affiliate News](#)
- [Africa](#)
- [Amazon](#)
- [AML](#)
- [Artificial Intelligence](#)
- [Attorney-Client Privilege](#)
- [Banks](#)
- [Biometric](#)
- [Blockchain](#)
- [Brazil](#)
- [Breach Notification](#)

We're Online!
How may I help you today?



- Inventory the types of data stored, processed or transmitted by the software, and the safeguards applicable to each data type.

CONFORMITY ASSESSMENT CRITERIA

The White Paper defines criteria for a Supplier's Declaration of Conformity. The declaration of conformity is intended to "provide written assurance of conformity to the specified requirements."

To meet the conformity assessment criteria, software providers will need to implement the following practices:

- Maintain procedures for issuing, maintaining, extending, reducing, suspending or withdrawing the declaration and the label attestations.
- Maintain procedures to ensure "continued conformity" with the label attestations.
- Separation of responsibilities and roles between the person conducting the review of the attestation and the signatory of the consumer software attestation.
- If the declaration was issued by an accredited laboratory or inspection body, maintain the results of the assessment and other supporting documentation that identifies the third-party and its qualifications, including accreditation status.

LABELING CRITERIA

The White Paper recommends a single, consumer-tested label which indicates that the software has met the technical and conformity assessment criteria. The label may also provide a means for consumers to access additional online information, including:

- Consumer-focused information about the labeling program;
- The declaration of conformity; and
- Descriptions supporting the data inventory and protection attestations.

AREAS FOR COMMENT

NIST requests comments on "all aspects of the criteria," including:

- Whether the criteria will achieve the goals of the EO by increasing consumer awareness and improving the cybersecurity of consumer software.
- Whether the criteria will enable and encourage software providers to improve the cybersecurity of their products and the information they make available to consumers.
- Whether the label should include a definitive statement that "the software product meets the NIST baseline technical criteria."
- Whether the software label approach and design should be similar to the forthcoming IoT product label "to facilitate brand recognition."
- Whether to include "more details on evidence required to support assertions."
- Whether to provide a template Declaration of Conformity.
- Whether the technical baseline criteria are appropriate, including the "feasibility, clarity, completeness, and appropriateness of attestations."

PRACTICE NOTES

Consumer software providers should consider whether they would benefit from labeling their software as NIST-compliant, and, if so, whether they could meet the requirements for secure development, information disclosure and conformity declaration. NIST is accepting comments on the draft through December 16, 2021.

This article is authored by [Todd McClelland](#), [Shawn Helms](#), and [Robert Duffy](#) from [McDermott Will & Emery](#). We received permission from the firm to republish the article for the ADCG community. The original post can be found [here](#).

Share This



Related Posts



Implementing the NIST Privacy Framework – Govern Function

The National Institute of Standards and Technology (NIST) Privacy Framework is a widely known control set used to assist organizations in identifying privacy risks within their business environment and allocating resources to mitigate these risks. Our team previously published an article



The Impact of Data Security Incident Trends on Commercial Transactions

The 2021 edition of BakerHostetler's annual Data Security Incident Response Report – a report based on the firm's experience with data security incident response and litigation over the past year – features a number of



Synopsis of Recently Passed New York State Laws on Cybersecurity


Two new privacy protection laws were signed into law by New York Governor Andrew Cuomo on July 25, 2019. (NY State Law S.5575B/A.5635 – or SHIELD Act – "Imposes Stronger Obligations on Businesses Handling Private Customer Data to Provide Proper Notification of Security

<input type="checkbox"/>	Breach prevention
<input type="checkbox"/>	Breach response
<input type="checkbox"/>	Broker Dealers
<input type="checkbox"/>	Business
<input type="checkbox"/>	Business Continuity
<input type="checkbox"/>	C-Suite
<input type="checkbox"/>	California
<input type="checkbox"/>	Canada
<input type="checkbox"/>	CCPA
<input type="checkbox"/>	CDPA
<input type="checkbox"/>	Certificate Course
<input type="checkbox"/>	Chamber of Commerce
<input type="checkbox"/>	Charter Member Spotlight
<input type="checkbox"/>	China
<input type="checkbox"/>	CIO
<input type="checkbox"/>	CISA
<input type="checkbox"/>	CISO
<input type="checkbox"/>	Class Actions
<input type="checkbox"/>	CMMC
<input type="checkbox"/>	CMO
<input type="checkbox"/>	CNIL
<input type="checkbox"/>	Collective Redress Directive
<input type="checkbox"/>	Colorado
<input type="checkbox"/>	Commerce Department
<input type="checkbox"/>	Compliance
<input type="checkbox"/>	Congress
<input type="checkbox"/>	Consumer Privacy
<input type="checkbox"/>	Consumer Software
<input type="checkbox"/>	Cookies
<input type="checkbox"/>	COPPA
<input type="checkbox"/>	Courts
<input type="checkbox"/>	COVID-19
<input type="checkbox"/>	CPRA
<input type="checkbox"/>	Cross-Border Data Transfers
<input type="checkbox"/>	Cryptocurrency
<input type="checkbox"/>	Cyber Fraud
<input type="checkbox"/>	Cybercrime
<input type="checkbox"/>	Cybersecurity
<input type="checkbox"/>	Dark Patterns
<input type="checkbox"/>	Data Breach
<input type="checkbox"/>	Data Brokers
<input type="checkbox"/>	Data Controllers
<input type="checkbox"/>	Data Disposition
<input type="checkbox"/>	Data Governance
<input type="checkbox"/>	Data Mapping and Inventory
<input type="checkbox"/>	Data Privacy
<input type="checkbox"/>	Data Protection
<input type="checkbox"/>	Data Protection Agency
<input type="checkbox"/>	Data Retention
<input type="checkbox"/>	Data Rights Management (DRM)
<input type="checkbox"/>	Data Security
<input type="checkbox"/>	Data Sharing
<input type="checkbox"/>	Data Stewardship


We're Online!
How may I help you today?




outlining the best ways to leverage the NIST Privacy (NIST-P) Framework to assess data privacy posture,...

 Become a member to access this content.

important insights previously covered on this blog including trends in global breach notification, healthcare industry risks and ransomware. The Report is a helpful tool for companies...

 Become a member to access this content.

Breaches.”). The law takes effect 240 days from the date of signing...

 Become a member to access this content.

Leave a Reply

You must be [logged in](#) to post a comment.

- Data Subjects
- data trusts
- Department of Justice
- DHS
- differential privacy
- Digital Identity
- Digital Payments
- DPA 1998
- DPO
- Dubai
- European Union
- Executive Order
- Export License
- Federal Agencies
- Federal Communications Commission
- Federal Reserve
- Federal Trade Commission (FTC)
- Federated Learning
- Financial Services
- FINRA
- FinTech
- France
- GDPR
- Genetic Information
- GLBA
- Governance
- Government Contracting
- Hiring
- Hybrid
- Illinois
- India
- International Agreements
- Investigations
- IT
- Japan
- Legislation
- Litigation
- Live Webinar
- Lobbying
- Machine Learning
- Marketing
- Maryland
- Members Only
- New York
- New York State
- NIST
- North Carolina
- OFAC
- Op-Ed
- Organization Structure
- PDPL
- Penalties and Enforcement
- Pennsylvania

We're Online!
How may I help you today?



- Personal Information
- Personally Identifiable Information (PII)
- Phishing
- PIPL
- Podcast
- Press Release
- Privacy
- Privacy by Design
- Privacy Rights Request
- Privacy Shield
- Project Management
- RACI
- Ransomware
- Recordings Available
- Resilience
- Resources
- Risk Management
- Safeguards Rule
- Sanctions
- Saudi Arabia
- SEC
- Senate
- Spyware
- State Laws
- Supply Chains
- Surveillance
- Switzerland
- Technology
- Telecommunications Infrastructure
- Third Party Compliance
- Training and Education
- UAE
- Uncategorized
- United Kingdom
- US Data Privacy Legislation
- US Regulatory
- Utah
- Virginia
- Weekly Update
- Work from Home



FOLLOW US



Search

MENU

Membership
Training
News & Resources
Conferences
Affiliate Members

LEGAL

Terms & Conditions
Privacy Policy
Cookie Policy

Login

We're Online!
How may I help you today?



