

Defining the requirement of “reasonable security” in recently effective and pending federal and state consumer data privacy laws

Presented at the  
*2022 ESSENTIAL CYBERSECURITY LAW CONFERENCE*  
by  
Elizabeth Rogers, CIPP/US  
July 27, 2022

1

1

## Agenda: Let's Get Reasonable!

---

\*Enters password\*  
"Incorrect password"  
"Incorrect password"  
"Incorrect password"  
\*Resets password\*  
"New password cannot  
be your old password"



2

2

## Agenda

- High level review of Federal reasonable security requirements of President Biden's Executive Order, the FTC and pending American Data Privacy Protection ACT, among other federal legislation and regulation
- State privacy laws and separate pending and effective requirements for establishing a reasonable security program
- Key Developments
- Legal Requirements
- Key Affirmative Security Requirements
- Case studies to help understand what regulators consider to be a reasonable security program

# Federal Overview

## POTUS Announces “reasonable security standards”

1. **Biden’s June 2021 Best Practices Memo: “What we urge you to do to protect against the threat of Ransomware”**
  - Implement best practices from the President’s Executive Order 14028
    - Multifactor Authentication (because passwords alone are routinely compromised)
    - Endpoint detection and response (to hunt for malicious activity on a network and to block it)
    - Encryption (so if data is stolen, it is unusable)
    - Skilled empowered security team (to patch rapidly, and share and incorporate threat information in your defenses)
2. **Backup your data, system images, and configurations, regularly test them, and keep the backups offline**

## POTUS Announces “reasonable security standards”

3. **Update and Patch Systems Promptly:** This includes maintaining the security of operating systems, applications and firmware, in a timely manner
4. **Test your Incident Response Plan:** There’s nothing that shows gaps in plans better than testing them
5. **Check your Security Team’s work:** Use a 3rd party pen tester to test the security of your systems and your ability to defend against a sophisticated attack
6. **Segment your networks:** There’s been a recent shift in ransomware attacks – from stealing data to disrupting operations

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](https://utcle.org/elibrary)

Title search: Reasonable Security Standards Taking Effect in 2023

Also available as part of the eCourse

[2022 Essential Cybersecurity Law eConference](#)

First appeared as part of the conference materials for the  
2022 Essential Cybersecurity Law session

"Reasonable Security Standards Taking Effect in 2023"