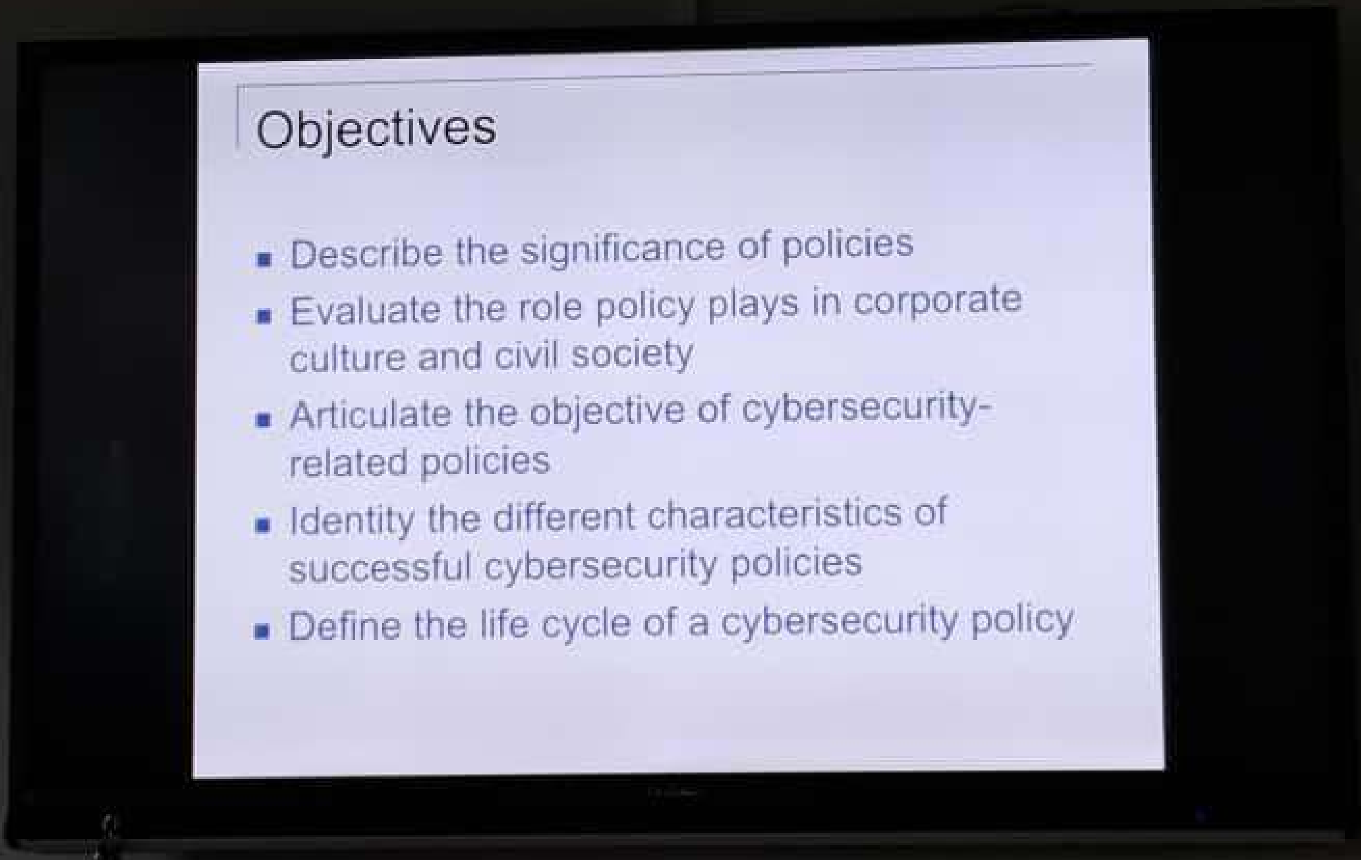
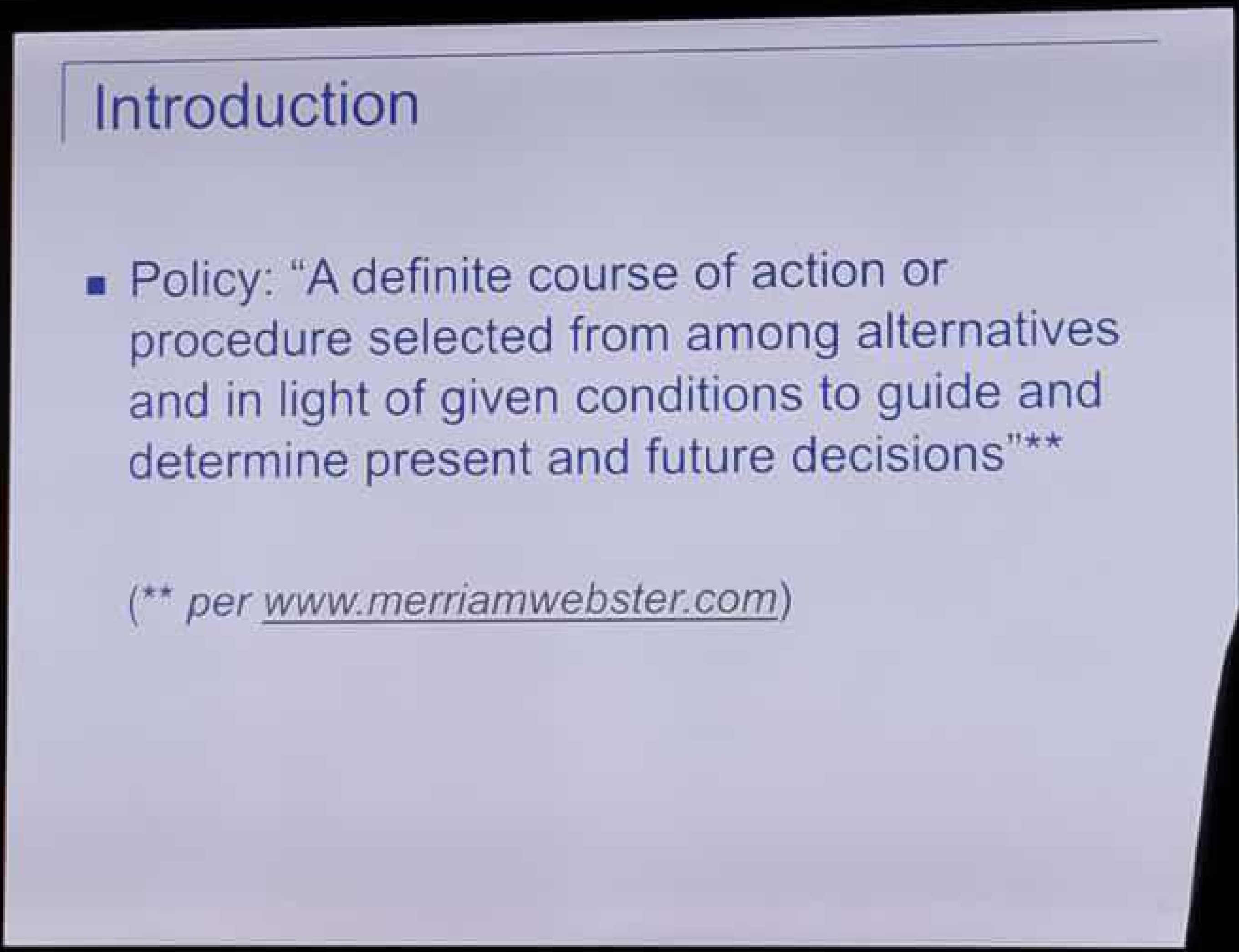


# Objectives

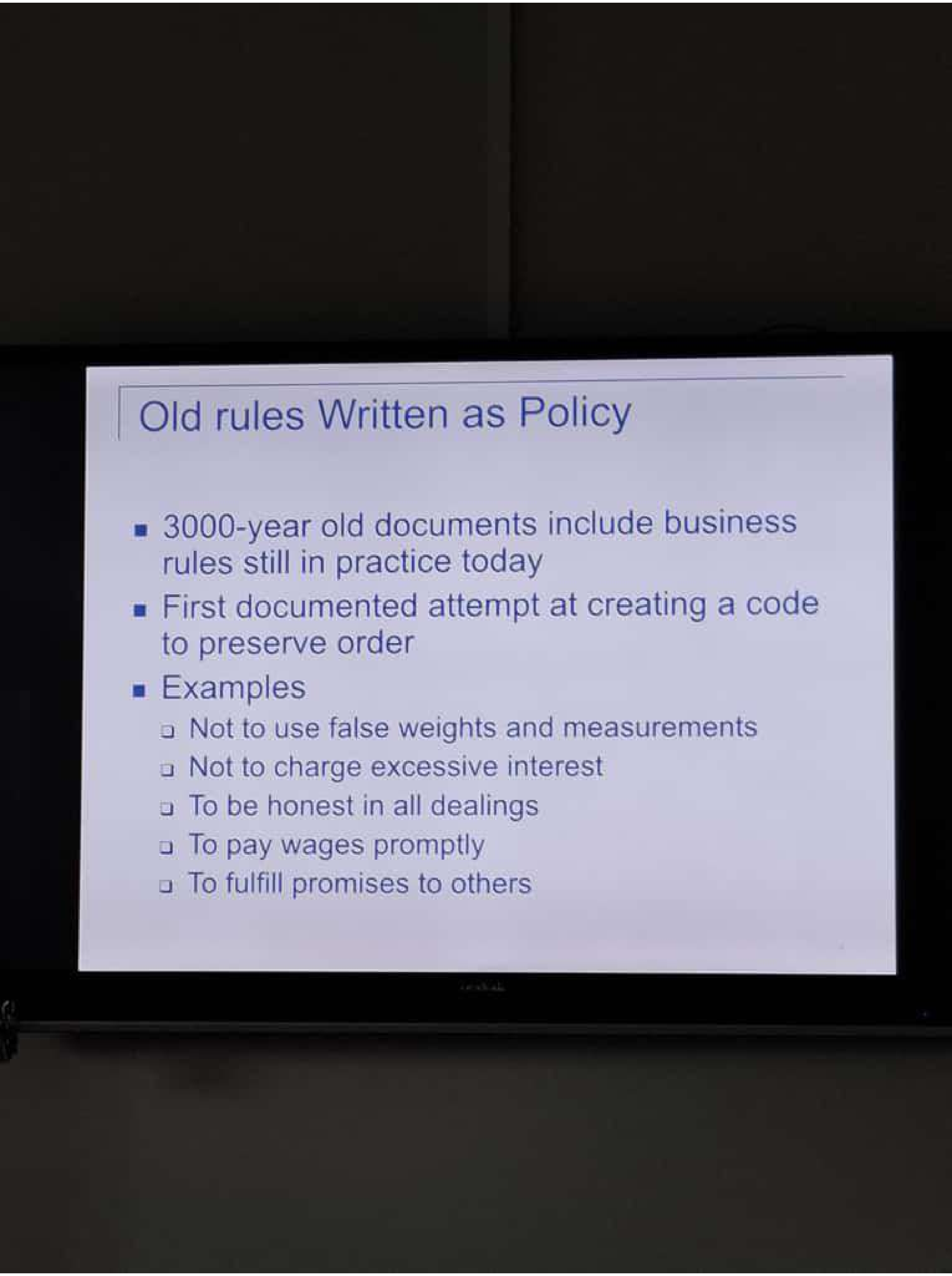
- Describe the significance of policies
- Evaluate the role policy plays in corporate culture and civil society
- Articulate the objective of cybersecurity-related policies
- Identity the different characteristics of successful cybersecurity policies
- Define the life cycle of a cybersecurity policy



## Introduction

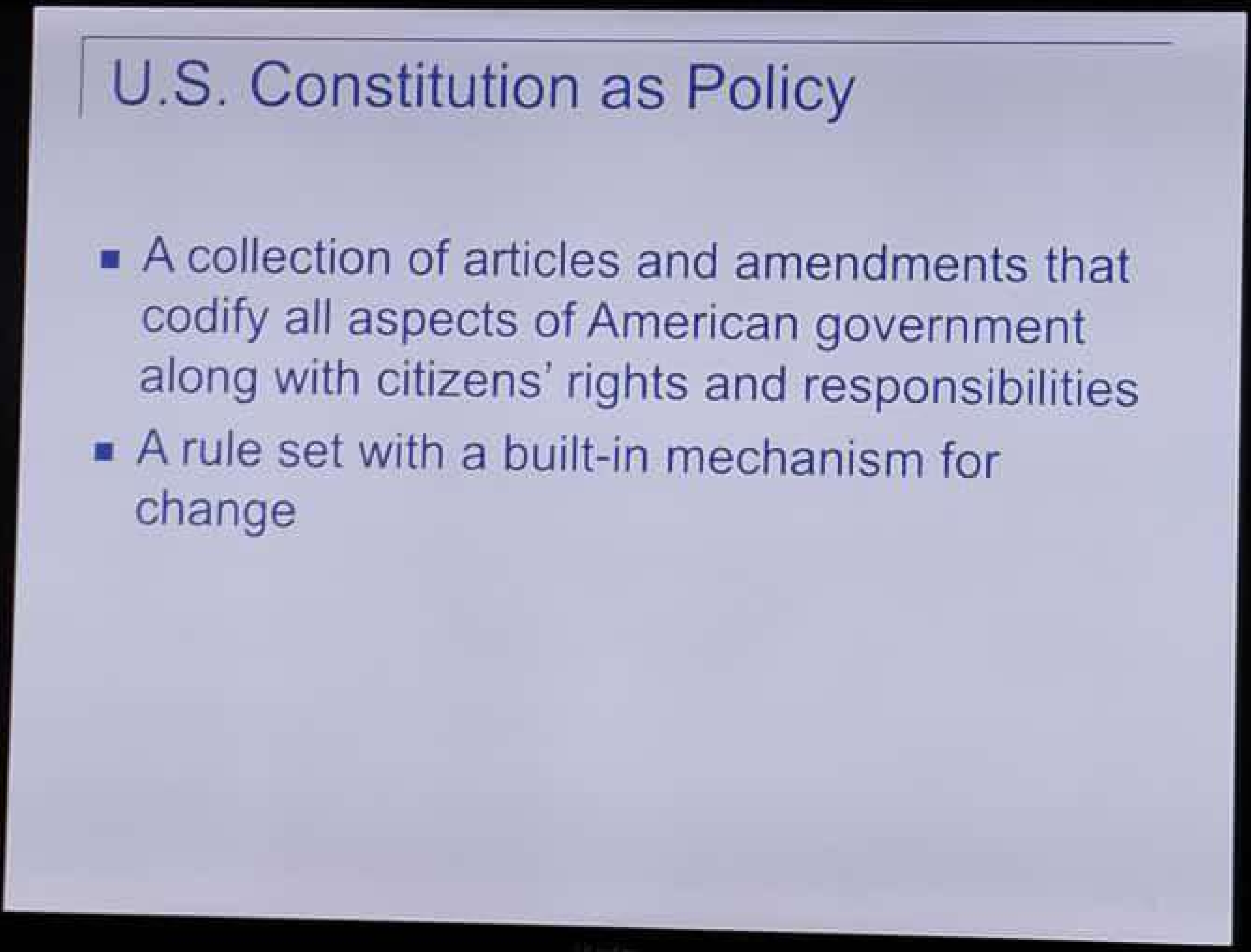
- Policy: “A definite course of action or procedure selected from among alternatives and in light of given conditions to guide and determine present and future decisions”**

(** *per www.merriamwebster.com*)



# Old rules Written as Policy

- 3000-year old documents include business rules still in practice today
- First documented attempt at creating a code to preserve order
- Examples
  - ❑ Not to use false weights and measurements
  - ❑ Not to charge excessive interest
  - ❑ To be honest in all dealings
  - ❑ To pay wages promptly
  - ❑ To fulfill promises to others

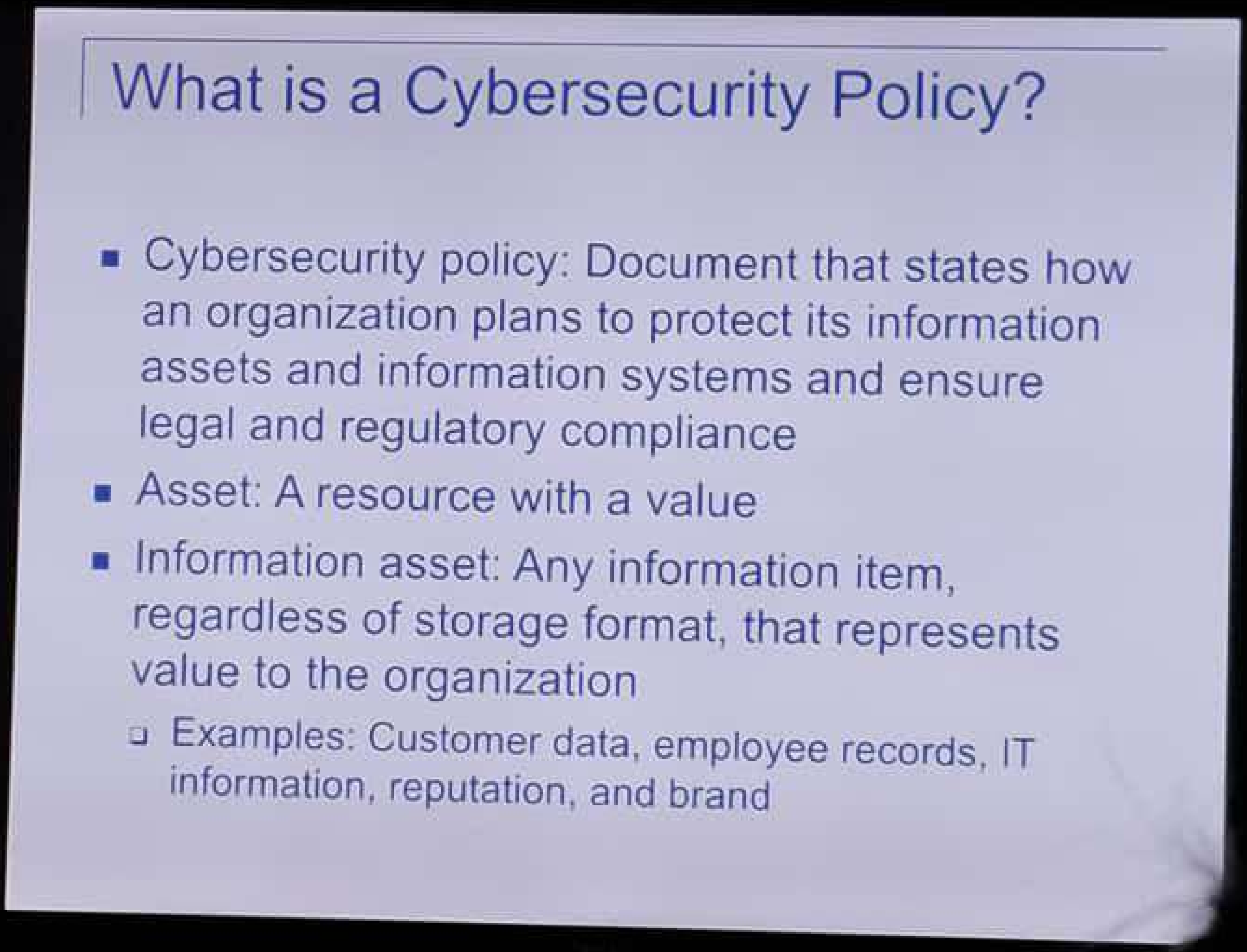


# U.S. Constitution as Policy

- A collection of articles and amendments that codify all aspects of American government along with citizens' rights and responsibilities
- A rule set with a built-in mechanism for change

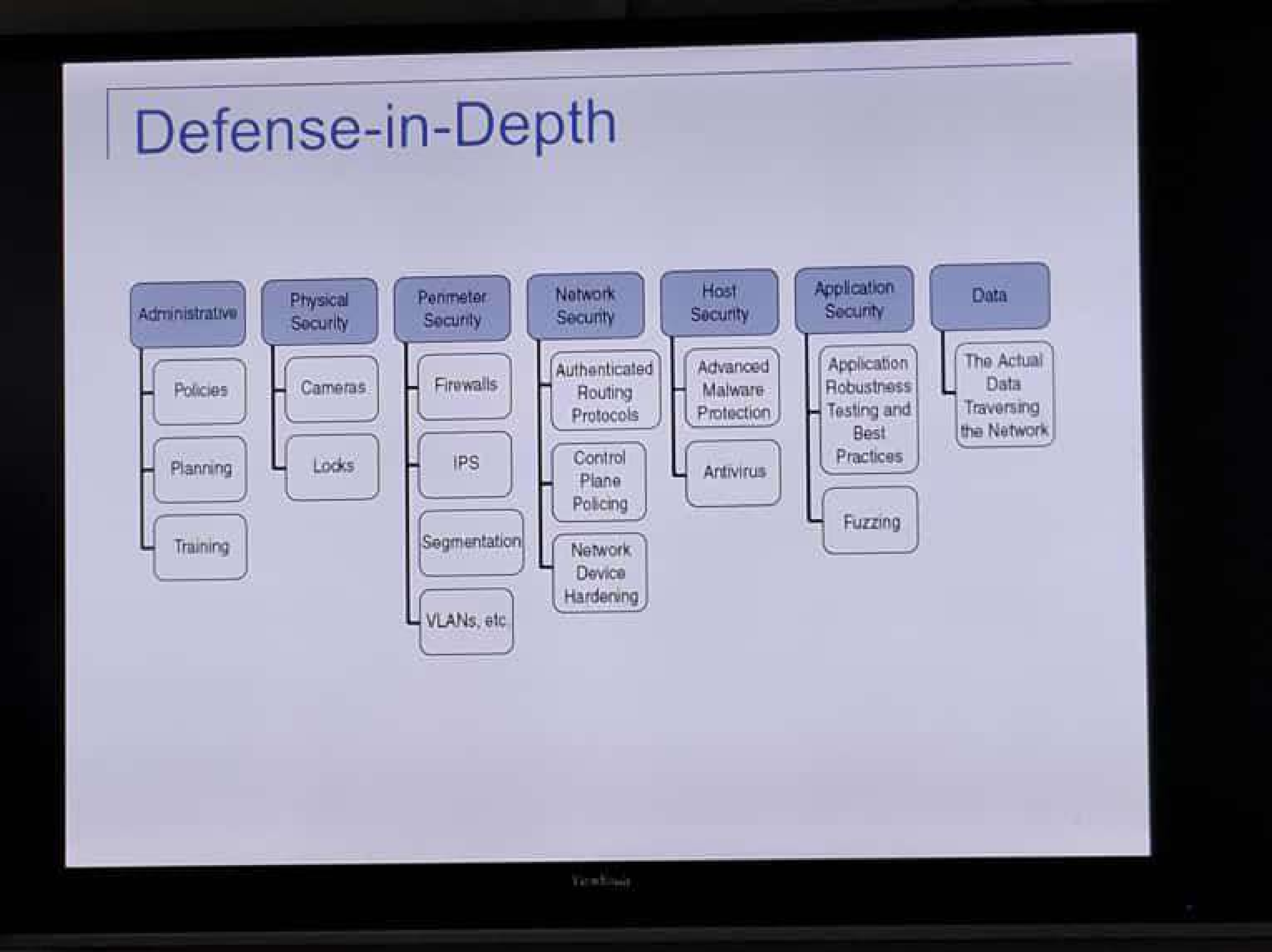
# Policy Today

- Corporate culture
  - Shared attitudes, values, goals, and practices that characterize a company
  - Three classifications
    - Negative
    - Neutral
    - Positive
- Guiding principles
  - Reflect the corporate culture



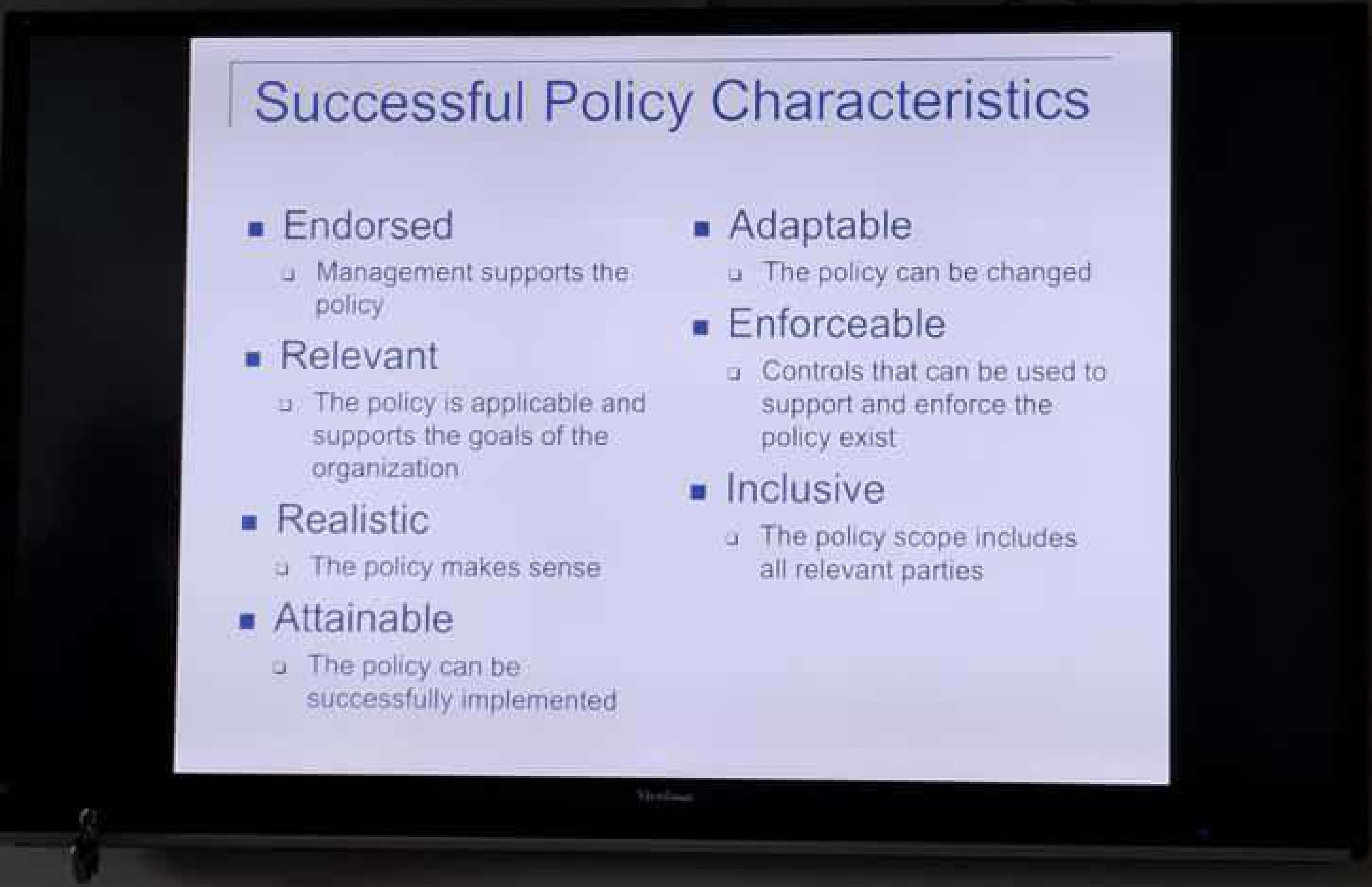
# What is a Cybersecurity Policy?

- Cybersecurity policy: Document that states how an organization plans to protect its information assets and information systems and ensure legal and regulatory compliance
- Asset: A resource with a value
- Information asset: Any information item, regardless of storage format, that represents value to the organization
  - Examples: Customer data, employee records, IT information, reputation, and brand



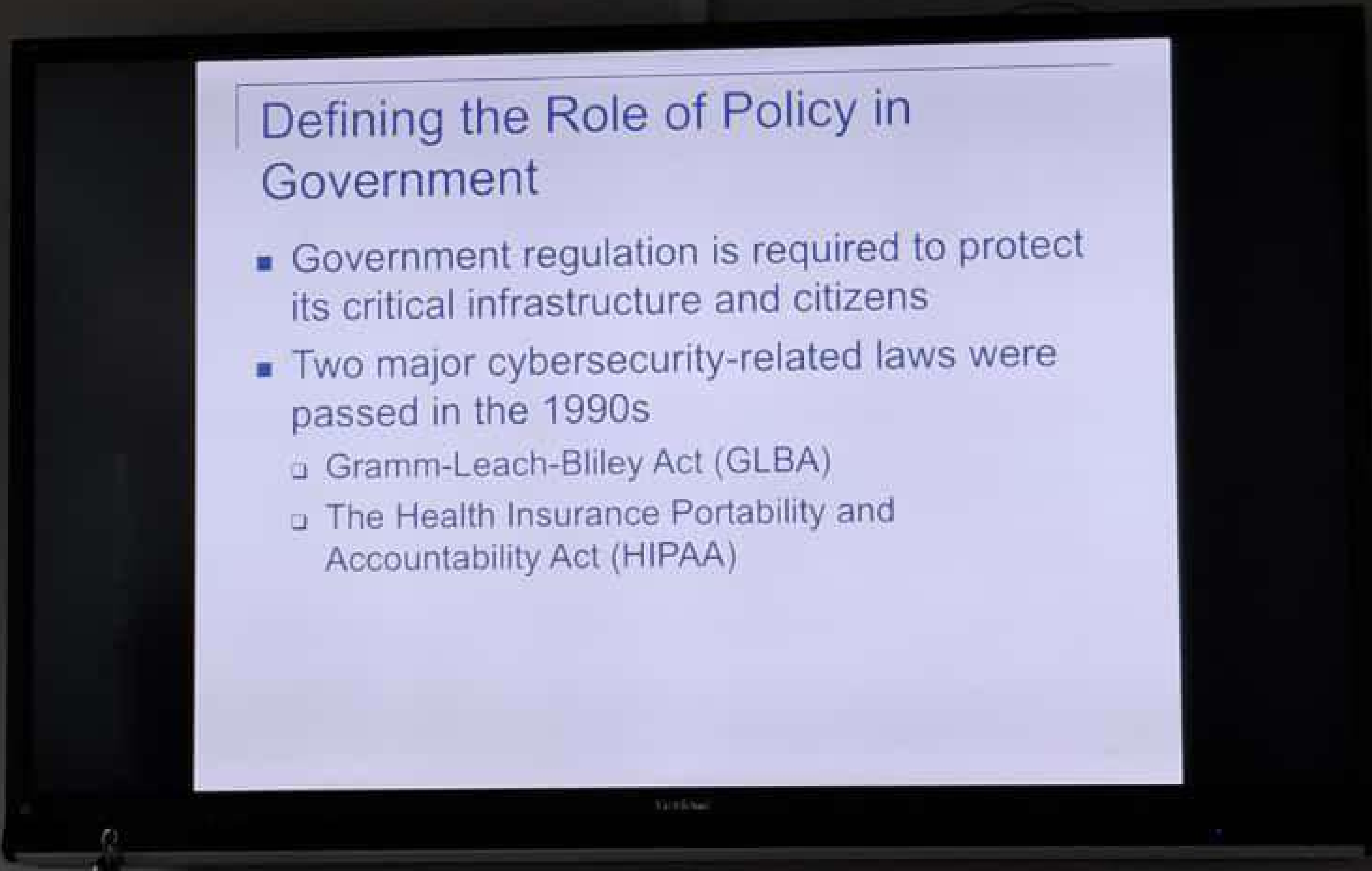
# Defense-in-Depth

- Administrative
  - Policies
  - Planning
  - Training
- Physical Security
  - Cameras
  - Locks
- Perimeter Security
  - Firewalls
  - IPS
  - Segmentation
  - VLANs, etc
- Network Security
  - Authenticated Routing Protocols
  - Control Plane Policing
  - Network Device Hardening
- Host Security
  - Advanced Malware Protection
  - Antivirus
- Application Security
  - Application Robustness Testing and Best Practices
  - Fuzzing
- Data
  - The Actual Data Traversing the Network



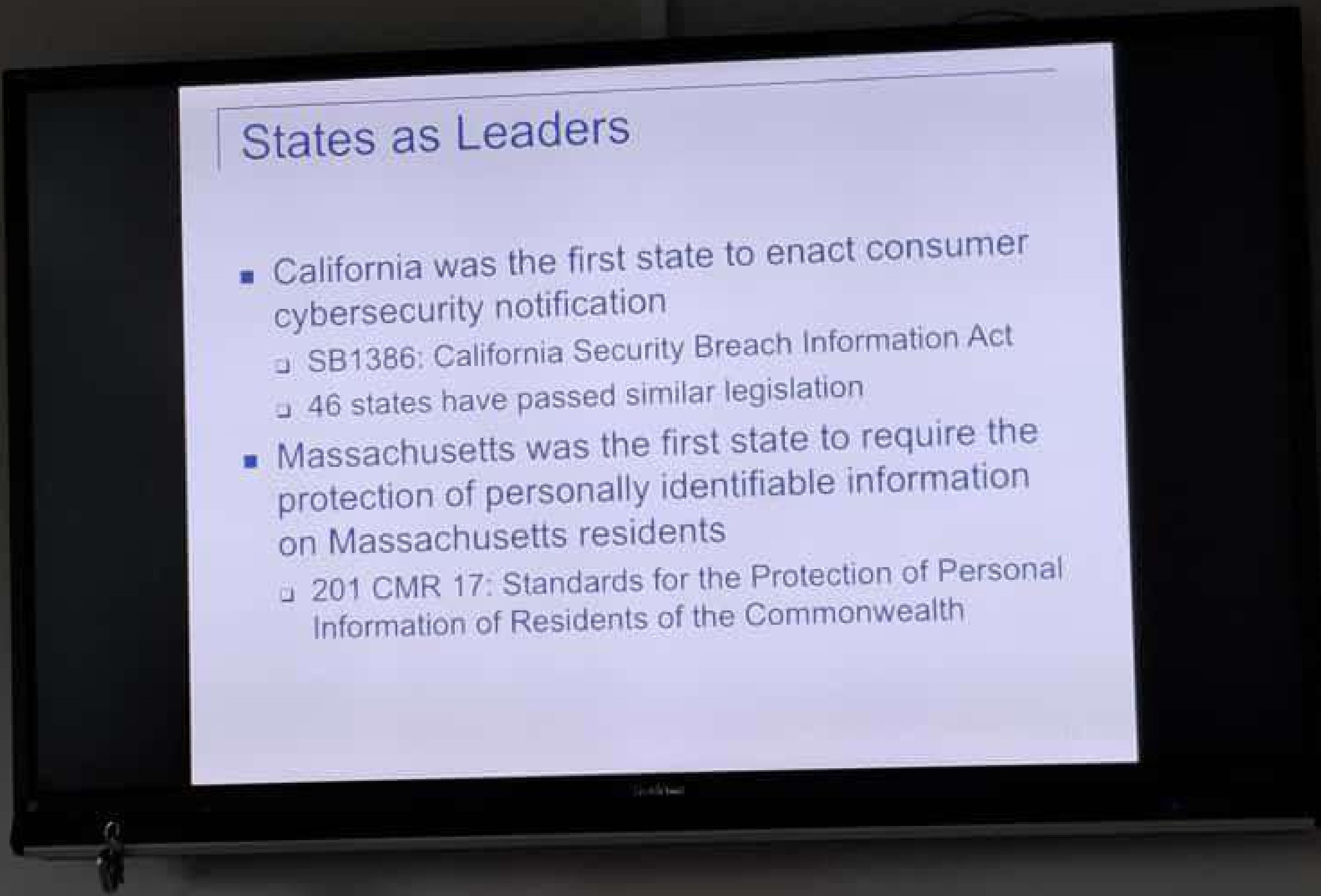
# Successful Policy Characteristics

- Endorsed
  - Management supports the policy
- Relevant
  - The policy is applicable and supports the goals of the organization
- Realistic
  - The policy makes sense
- Attainable
  - The policy can be successfully implemented
- Adaptable
  - The policy can be changed
- Enforceable
  - Controls that can be used to support and enforce the policy exist
- Inclusive
  - The policy scope includes all relevant parties



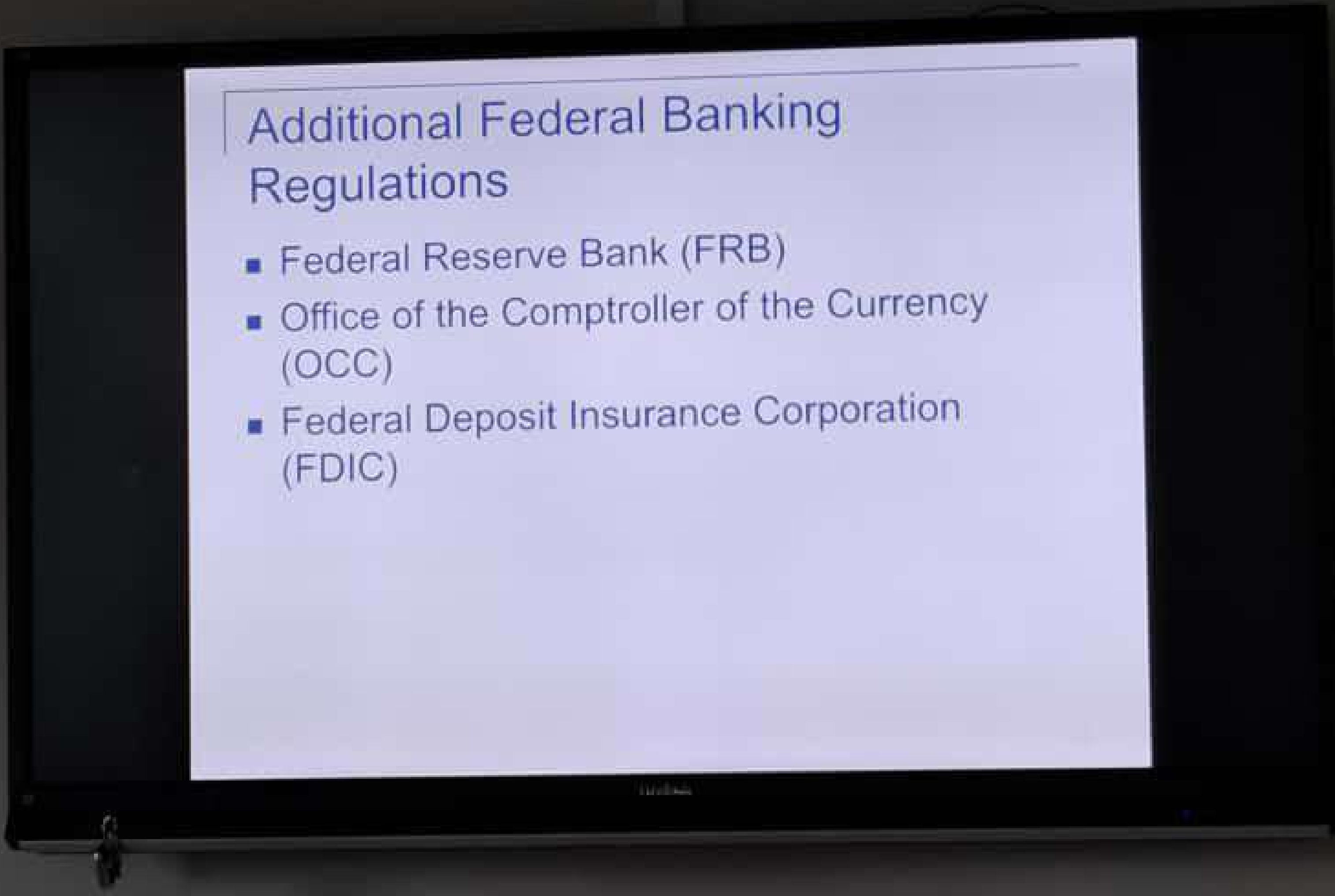
# Defining the Role of Policy in Government

- Government regulation is required to protect its critical infrastructure and citizens
- Two major cybersecurity-related laws were passed in the 1990s
  - Gramm-Leach-Bliley Act (GLBA)
  - The Health Insurance Portability and Accountability Act (HIPAA)



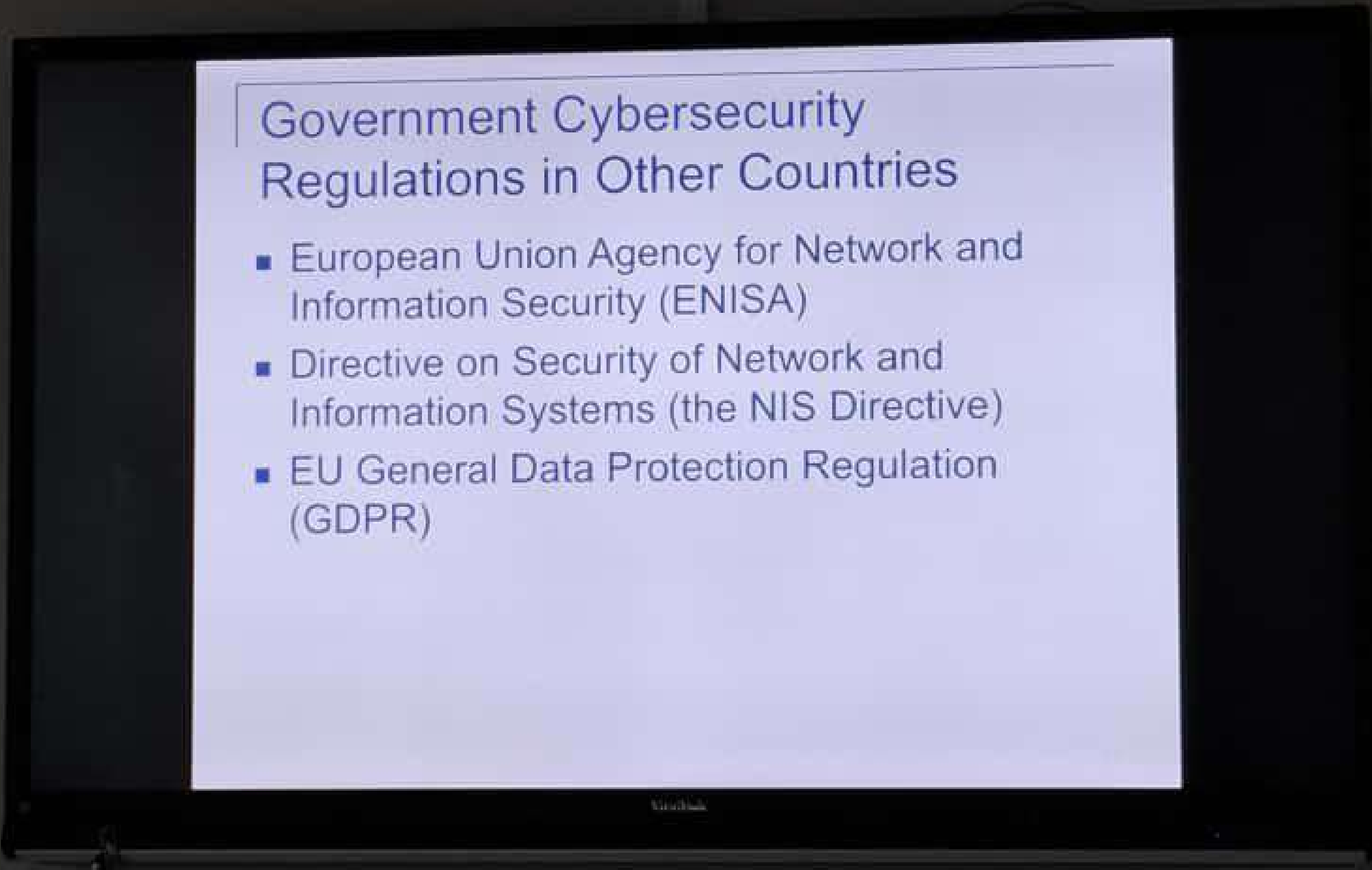
## States as Leaders

- California was the first state to enact consumer cybersecurity notification
  - ❑ SB1386: California Security Breach Information Act
  - ❑ 46 states have passed similar legislation
- Massachusetts was the first state to require the protection of personally identifiable information on Massachusetts residents
  - ❑ 201 CMR 17: Standards for the Protection of Personal Information of Residents of the Commonwealth



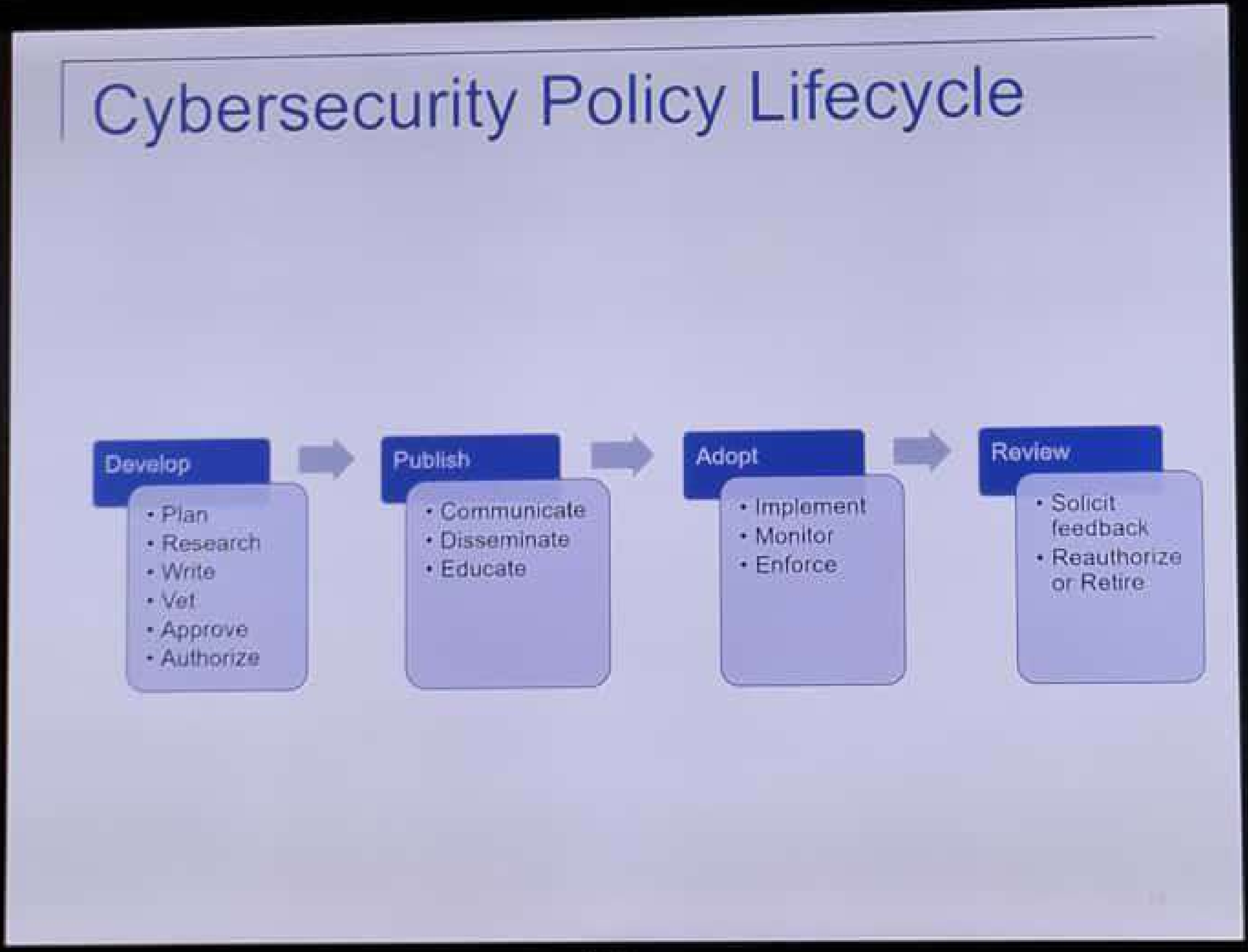
# Additional Federal Banking Regulations

- Federal Reserve Bank (FRB)
- Office of the Comptroller of the Currency (OCC)
- Federal Deposit Insurance Corporation (FDIC)



## Government Cybersecurity Regulations in Other Countries

- European Union Agency for Network and Information Security (ENISA)
- Directive on Security of Network and Information Systems (the NIS Directive)
- EU General Data Protection Regulation (GDPR)



# Cybersecurity Policy Lifecycle

**Develop**

- Plan
- Research
- Write
- Vet
- Approve
- Authorize

**Publish**

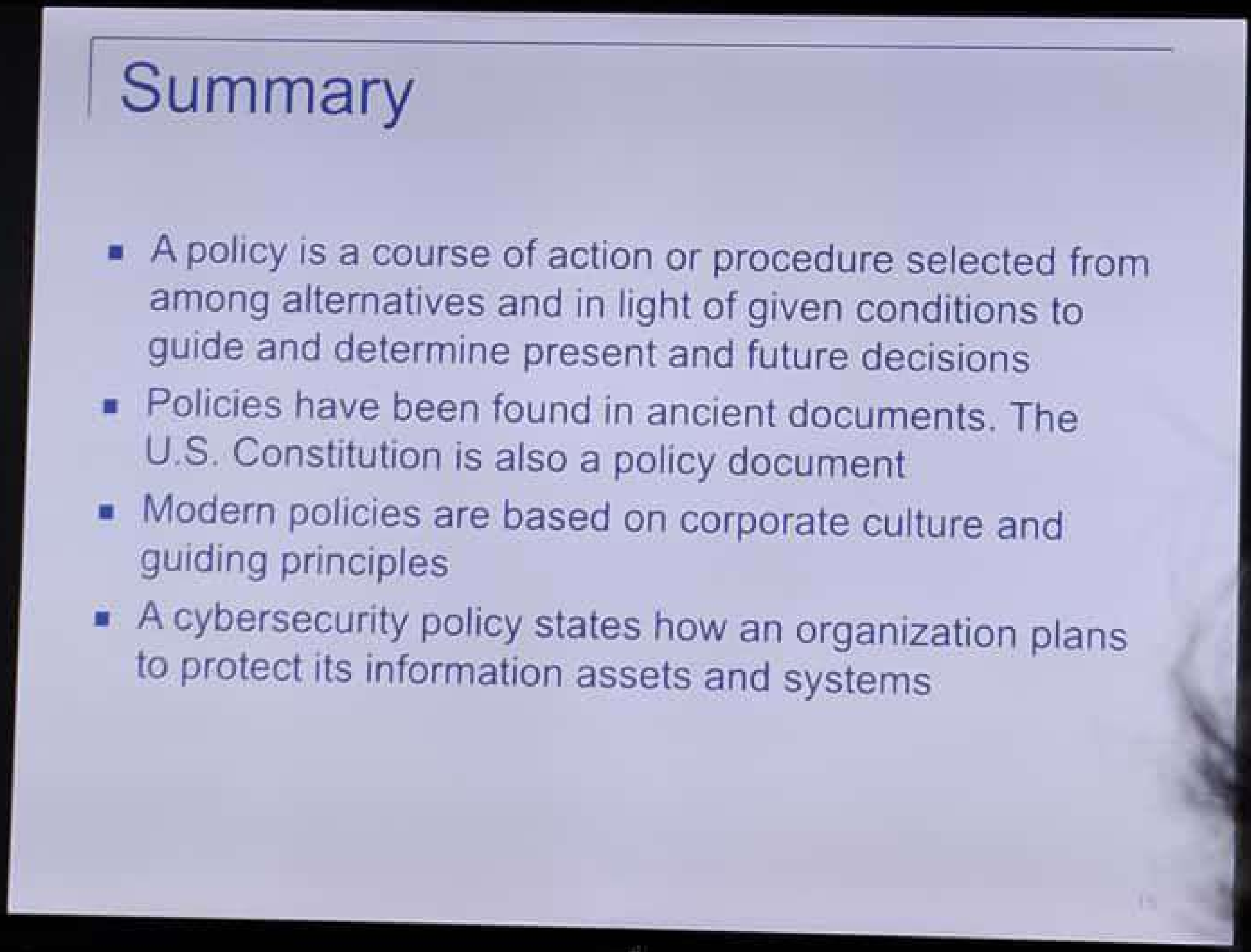
- Communicate
- Disseminate
- Educate

**Adopt**

- Implement
- Monitor
- Enforce

**Review**

- Solicit feedback
- Reauthorize or Retire



# Summary

- A policy is a course of action or procedure selected from among alternatives and in light of given conditions to guide and determine present and future decisions
- Policies have been found in ancient documents. The U.S. Constitution is also a policy document
- Modern policies are based on corporate culture and guiding principles
- A cybersecurity policy states how an organization plans to protect its information assets and systems