

# Federal Information Security Modernization Act (FISMA, 2002):

- Team Lead: Cavan Lawes
- Lead Researcher: Valentina Giraldo
- Lead Presenter: Amadeus Saez
- Second presenter: Sofia Mazumdar
- Team Collaborators:

Gustavo Gambaro & Jan-Carlos



# OUTLINE

- **Slide 3.....** History and context of the law  
(Why was it necessary?)
- **Slide 4.....** Key provisions and regulations related to cybersecurity (What is the Law?)
- **Slide 5.....** Real-world case studies illustrating its impact (Active or concluded cases)
- **Slide 6.....** Business and Societal Impacts of the Law
- **Slide 7.....** How the Law can be improved  
(Due to consequences)
- **Slide 8.....** Conclusion

# History and Context of the Law

- Created in December of 2002
- Title III of the E-government act (2002), part of a larger law being passed
- It was needed to defend against the increasing number of cyberattacks
- As security standard FISMA was used to keep up with technology
- Enacted by congress and enforced by DHS in collaboration with OMB, and NIST cybersecurity framework
- Department of defense (DoD) and department of veteran affairs (VA) was infiltrated
- Solar Sunrise incident in 1998: attackers gained access to the DoD
- Hackers downloading passwords and uploading trap doors to military computers



# Key Provisions and Regulations Related to Cybersecurity



- FISMA is the federal information and security Modernization act
- U.S law stating the information security standards required in all U.S Federal agencies
- FISMA Established a framework for securing federal government information/systems
- Key requirements/Basic security controls:
  - Risk management/assessment
  - Security plan
  - Continuous monitoring
  - Incident response and report



# Real-world Case Studies Illustrating its Impact

## The data breach at the Office of Personnel Management (OPM) in 2015:

- The attack exposed federal employees' personal information
  - Exposed weaknesses in the federal government's information security practices.
  - Federal agencies changed cybersecurity measures to meet FISMA standards
- 
- Veterans Affairs Data Breach:
  - An information breach (2006) exposing personal data of many veterans/ military personnel
  - A laptop of an on-duty military officer was stolen exposing personal information
  - It had high media coverage and made the public lose trust

# Business and Societal Impacts of the Law

## Business impacts

- Increased security protocols:
  - Those interacting with government agencies must comply with FISMA standards
- Increased cost
- Client trust and opportunities:  
working with governments complying with FISMA shows reliability and security

## Societal impacts

- Trust in government services
- Enhanced protection of information
- Cybersecurity awareness



# How the Law can be Improved

## Suggestions for improvement:

- Modernize FISMA policies as technology increases (AI)
- Use more automated systems for advanced monitoring
- Improve incident response capabilities
- Invest in new technology
- Enhance collaboration and information sharing among federal agencies
- More resources for training and education on cybersecurity
- As technology improved so did FISMA which was amended in 2014

## Consequences:

- Improved security
- Increased accountability and transparency in federal agencies' handling of information security

## **Non-FISMA compliance penalties:**

- Censure by congress, a reduction in federal funding, and reputational damage, loss of contracts
- While FISMA does not have any legal penalties, it could trigger actions from other laws





# Conclusion

- FISMA is the federal information and security modernization assessment act.
- U.S law stating that federal agencies security standards are required to protect secure information
- The Solar Sunrise incident in 1998, Veterans Affairs Data Breach, Office of Personnel Management (OPM) in 2015 all led to the implementation or enforcement of FISMA
- Due to this law it increased security and the handling of information security
- Many improvements can be made to FISMA:
- Better collaboration, Better education on security standards, and streamlining the security process for quicker and better results
- FISMA was created to provide accountability for the delivery of information security capabilities.



# Citation page

- <https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act>
- <https://www.ekransystem.com/en/solutions/meeting-compliance-requirements/fisma-compliance>
- <https://security.cms.gov/learn/federal-information-security-modernization-act-fisma>
- <https://www.digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more>
- <https://www.cio.gov/handbook/it-laws/fisma/>
- <https://www.bankinfosecurity.com/blogs/did-fisma-facilitate-opm-hack-p-1879>
- <https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act>
- [PLAW-107publ347.pdf](#)
- <https://www.congress.gov/bill/107th-congress/house-bill/3844#:~:text=Federal%20Information%20Security%20Management%20Act%20of%202002%20%2D%20Requires%20the%20Director,commensurate%20with%20the%20risk%20and>
- <https://www.sciencedirect.com/topics/computer-science/moonlight-maze>
- <https://www.bartleby.com/essay/Federal-Information-Security-Management-Act-F3M6YJGQ3FT85>
- <https://nsarchive.gwu.edu/document/22658-document-03-federal-bureau-investigation>

