# The Economics of Cybersecurity — Lecture 12 Notes

Adam Hastings

April 9, 2024

## 1 Alphabet Soup

- ONCD — Office of the National Cyber Director
  - Advisor to President; part of Executive Branch
  - Since 2021
  - Published National Cybersecurity Strategy
- CISA — Cybersecurity and Infrastructure Security Agency
  - Agency within the DHS (Deparment of Homeland Security, part of Executive Branch), whose mission is public security (things like anti-terrorism, border security, disaster response (FEMA), etc.)
  - Established 2018 (replaced older program)
  - Responsible for 1) ensuring federal cybersecurity, and 2) coordinating cybersecurity and infrastructure security programs within the US.
  - *Why does cybersecurity need coordination?* Central point for information sharing
  - Focused on improving the federal government's security but also the security of US companies and citizens.
- NIST — National Institute for Standards and Technology
  - Part of Department of Commerce
  - Formed in 1901
  - Make standards. *Ask: What's a standard?*
  - Example from their website: Firehoses and firehose fittings on fire hydrants are nationally standardized (in response to Great Baltimore Fire of 1904).
  - Standardizes many things
  - Reference Peanut Butter. Costs about $2000, *Why?* For testing laboratory equipment. Guaranteed to have an exact number of calories, protein, etc. so that food manufacturers can calibrate their equipment as part of food safety testing required by the FDA (Food and Drug Administration). (Example—NIST provides standards; NIST does not enforce standards!)

  - *Where is NIST big in cybersecurity (besides the NIST CSF)?* Cryptography! AES, SHA, RSA, DSA, ECDSA are all NIST standards. *Who knew this?* The standards describe exactly how the computation should be done. Even standards for how to generate random bits!
  - Current big thing is the move to Post-Quantum cryptography (Quantum breaks RSA!). Currently in final phase (about four remaining, doing more tests and getting input from cryptographers I suppose)

- Digression:
  - There are many, many standards in technology. Examples:
  - USB standard (USB Implementers Forum); Bluetooth (Bluetooth Special Interest Group); U2F/FIDO (FIDO Alliance); POSIX (IEEE); double-width precision floating points (IEEE)
  - These are not government bodies. Made up of self-interested companies.
  - *Why are some standards like cryptography standardized by the government while others are not?*

- There is clear interest in Washington in taking a more active hand in security. Unclear which agency this will come from...CISA does not pass regulations, and neither does NIST...maybe someone more keyed in would know what's happening behind the scenes (Jay Healy perhaps? Plug for his class!)

- Some non-regulatory agencies in the US:
  - USCYBERCOM — United States Cyber Command
    * **NOT** a regulatory agency. Part of the US Military, operating under the Department of Defense. Mission: cyberwarfare.
    * Founded 2010
    * Created as a defensive force; Probably better seen as an offensive force (e.g. take down ISIS servers/disrupt operations)
  - NSA — National Security Agency (1952). Purpose: Obtain intelligence, cyrptanalysis, SIGINT, data collection, Snowden Leaks, et cetera.
  - FBI, CIA do intelligence gathering as well (CIA is more focused on human intelligence though, FBI is kind of like federal police. Neither going to have an impact in national cybersecurity.)

# 2 National Cyberecurity Strategy

# 3 NIST Cybersecurity Framework

This is very much a **goal oriented** approach.

# 4 ENISA Cyber Resiliance Act