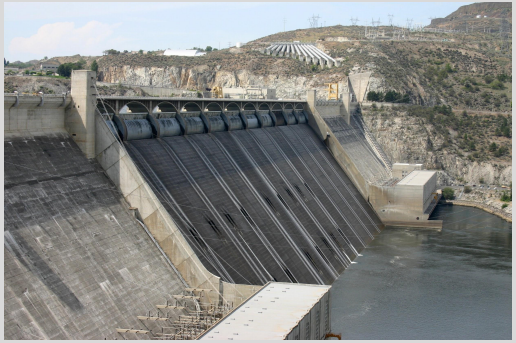
Cybersecurity - The Federal Response

The Federal Response Towards Cybersecurity Vulnerabilities, Analysis and Resolution Within The Obama Administration

Cybersecurity - The Federal Response

Protecting the National Infrastructure of Economic Activity and Value

- Airports, Seaports, Highways
- Electric Power Grids
- Dams, Aquifers and Reservoirs
- Railroads
- Sewer and Water lines
- Broadband and Fiber Optics
- Major Population Regions
- Conventions and Sporting Events
- Major Cultural Events
- The Internet



Cybersecurity - The Federal Response

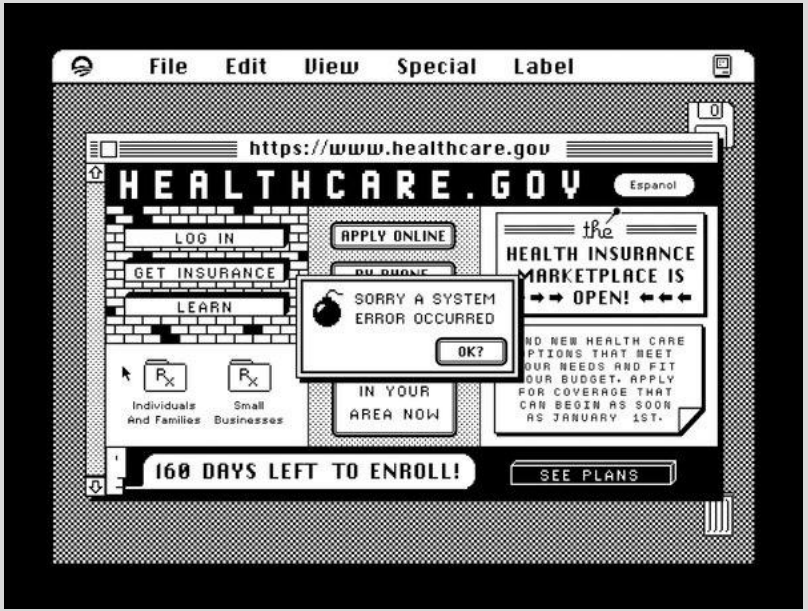
Executive Order 13636 (2/13) - Improving Critical Infrastructure Cybersecurity

- It is the **policy** of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.
- As used in this order, the term **critical infrastructure** means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters, (Section 2).
- Repeated cyber intrusions into critical infrastructure **demonstrate the need** for improved cybersecurity, (Section 1).

Cybersecurity - The Federal Response

Challenges - Healthcare.gov, WikiLeaks and Classified/Confidential docs.

- October 1, 2013 (two years ago!)
- Mismanagement of code and information
- **People are the greatest weakness!!!**



WIKILEAKS SCANDAL (“Cablegate”) - 2010

- 251,287 cables consist of 261,276,536 words
- Major embarrassment to top global leadership

EDWARD SNOWDEN - (2013)

- For better or for worse, leaked top secret info.

Cybersecurity - The Federal Response

Challenges - NSA/Edward Snowden (2013).

- PRISM - data surveillance program (2007 - present)
- Questions the fundamental relationship between a trusting public and a trusted government.
- Mixed public reaction: Democrats and liberals view Snowden as a traitor, while other conservative news outlets view Snowden as a patriot, set to expose the wrongdoings of the Obama Administration
- Found temporary asylum in Russia, where Putin and Obama enjoy a tense relationship.

Cybersecurity - The Federal Response

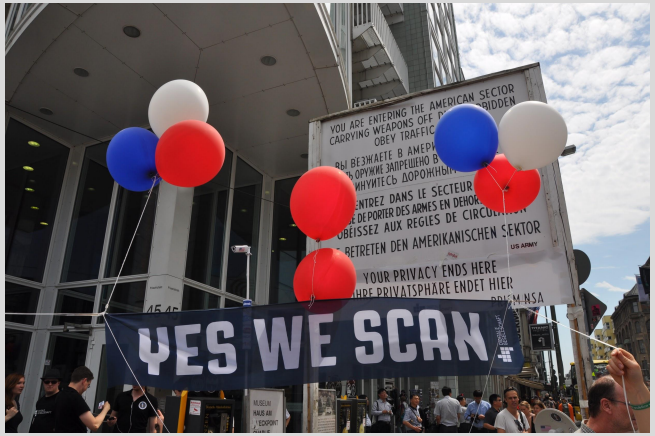
United States Cyber Command (USCYBERCOM)

- Armed forces sub-unified command under the command of the United States Strategic Command.
- Located in Fort Meade, Maryland, formed in 2009.
- Centralizes command of cyberspace operations, organizes existing cyber resources and synchronizes defense of U.S. military networks.
- 9EC4C12949A4F31474F299058CE2B22A
  - The MD5 hash of their mission statement!
  - (located on inner concentric roundel)

Cybersecurity - The Federal Response

Various Agencies Tasked With Cybersecurity

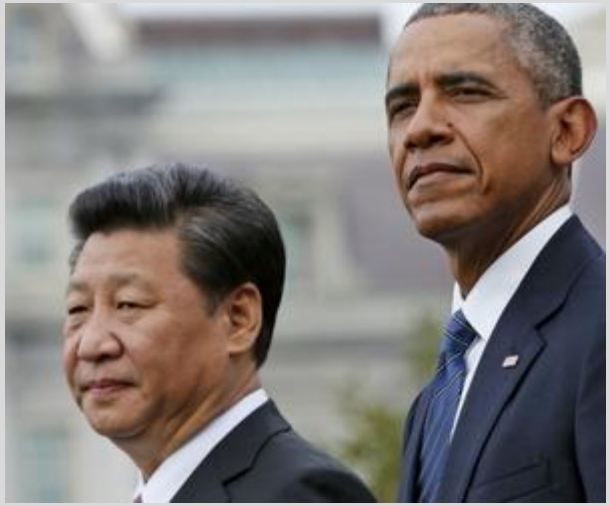
- Federal Bureau of Investigation (FBI)
- Central Intelligence Agency (CIA)
- Office of Personnel Management (OPM)
  - 2015 Breach - the estimate of the number of stolen records had increased to 21.5 million!
- Department of Defense (DOD)
- Department of Homeland Security (DHS, 2001 -)



Cybersecurity - The Federal Response

The Chinese Threat

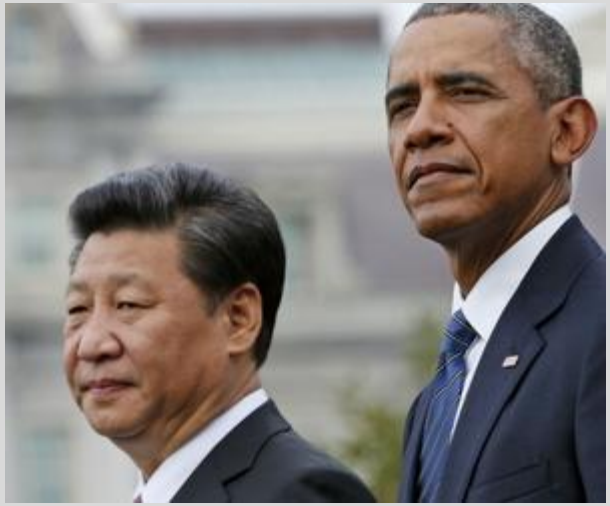
- Recent State Visit - September 24-25, 2015
- Pulled out all the pomp and circumstance of an official State Visit (fears of conflict due to a crushing debt)
  - "The Chinese government will not, in whatever form, engage in commercial theft or encourage or support such attempts by anyone. Both commercial cyber theft and hacking against government networks are crimes that must be punished in accordance with the law and relevant international treaties."
- Interesting because the Chinese government does not have to actively participate in the "commercial theft or espionage" in order to actually benefit from such theft or espionage.



Cybersecurity - The Federal Response

Conclusions:

1. A 21st century government should enjoy access to 21st century technology and national infrastructure.
2. This 21st century government needs to balance surveillance with citizen's privacy without abuse.
3. When surveillance abuses are found, take steps to resolve them immediately. Don't hide, classify, or kick down can to be resolved by a later presidential administration.
4. Only responsible use of national resources will guarantee an secure economy.



Cybersecurity - The Federal Response

Thank you. Are there any questions?