INFORMATION TECHNOLOGY LABORATORY

Case Study: Cybersecurity Framework

Impact on NIST's core research and measurement science

Agenda

- Context – Executive Order 13636 and the Cybersecurity Framework (CSF)
- About the Process
- Benefits and Opportunities
- Challenges
- Considerations
- Where are we today?

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

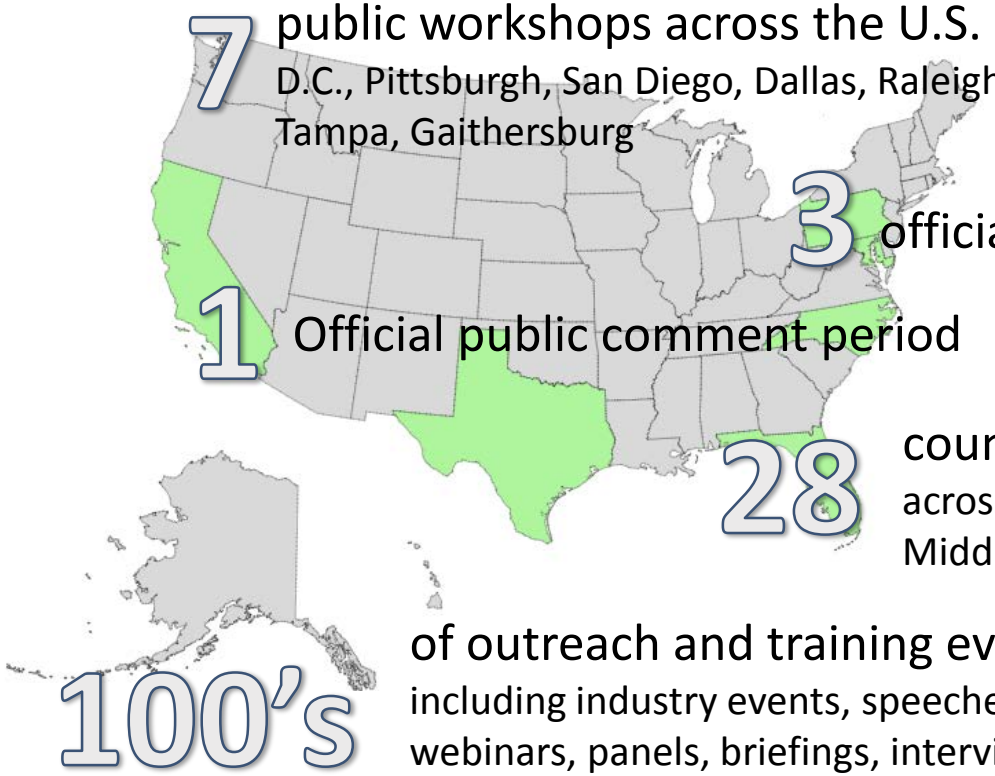
"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

President Barack Obama
Executive Order 13636, Feb. 12, 2013

- NIST was directed to work with stakeholders to develop a voluntary framework for reducing cybersecurity risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work

About the Process

Since February 2013:



7 public workshops across the U.S.
D.C., Pittsburgh, San Diego, Dallas, Raleigh, Tampa, Gaithersburg

3 official requests for information

1 Official public comment period

28 countries engaged
across the Americas, Asia, the Middle East, the EU, and all 5 Eyes

100's of outreach and training events
including industry events, speeches, webinars, panels, briefings, interviews, and testimonies

Benefits and Opportunities

- Strengthening long-standing collaborative relationships with industry
  - Ex, IT, Energy, Financial, Healthcare, Telecommunications
- Establishing new relationships, partnerships, and collaborations with new sectors and organizations
  - Ex, Maritime, Retail, Restaurants, Hospitality, Transportation
- Providing an opportunity to highlight our technical depth/breadth, and dedicated staff
- Amplifying awareness of and interest in other NIST cybersecurity programs
- Increasing our interactions with non-technical audiences
  - Ex, Industry Executives, Enterprise Risk Managers, Insurers, Auditors, Accountants, Legal

Challenges

- Diverted staff attention from other important work
  - ~120 cybersecurity staff; ~25 supported the CSF because of its importance
  - Ex, FISMA, Supply Chain, Privacy, Security Automation and Indicator Sharing, Secure BIOS
- Stretched staff throughout development (and beyond)
- Framework approach was different… should it be the norm?
- Interest continues to increase (important to set realistic expectations and manage to them)

Considerations

Does the initiative align with our mission and core capabilities?

Is there someone else that should do it, or that could do it better?

Do we understand and have the right assets, including “traditional” and “non-traditional” NIST skillsets, needed to carry out the program?

What level of impact is a successful outcome of the program expected to have?

Where are we today?

The value of our approach to public/private partnership is widely recognized

Our role and approach was reaffirmed in the Cybersecurity Enhancement Act of 2014

The Administration continues to turn to us on issues and initiatives of National importance

Interest in and use of the Cybersecurity Framework is strong… and growing!

Questions