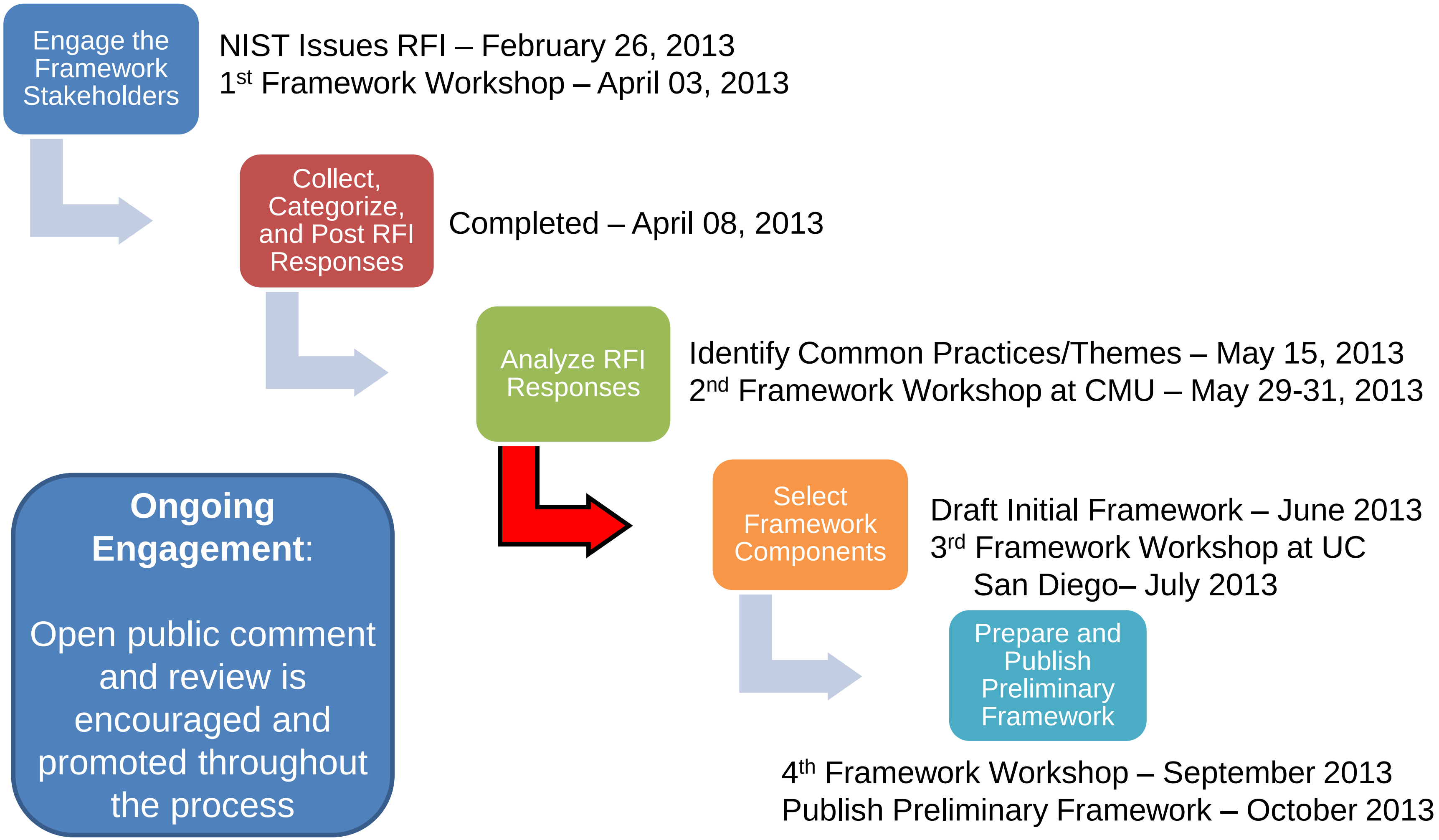
# 2nd Cybersecurity Framework Workshop

# Outbrief and
# Discussion of Next Steps

May 31, 2013

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

# Framework Development Process



Engage the Framework Stakeholders

NIST Issues RFI – February 26, 2013
1st Framework Workshop – April 03, 2013

Collect, Categorize, and Post RFI Responses

Completed – April 08, 2013

Analyze RFI Responses

Identify Common Practices/Themes – May 15, 2013
2nd Framework Workshop at CMU – May 29-31, 2013

Select Framework Components

Draft Initial Framework – June 2013
3rd Framework Workshop at UC
San Diego– July 2013

Prepare and Publish Preliminary Framework

4th Framework Workshop – September 2013
Publish Preliminary Framework – October 2013

**Ongoing Engagement**:

Open public comment and review is encouraged and promoted throughout the process

# Workshop Goals

- Further discussion of RFI inputs, current business/operational practices
- Refine and augment data set to be used in Initial Draft of Framework
- Shape the Properties and Characteristics of the Initial Draft Framework

The open and public review and comment process is directed by the President in the EO, AND is the right way to approach this development.

# What We Heard

The Framework should have the properties and characteristics:

- Not conflict with existing regulatory requirements
- Must have context for multiple audiences and relate to business drivers
- Modular approach to allow for differences in business
- Refer to existing frameworks, standards, guidelines, and practices

# Initial Workshop Conclusions

- Connection between Business / Mission Management and Cyber Risk Management is vital
  - Framework must support business decisions

- Cyber Risk Management – identify existing standards, guidelines, and common practices to support decisions in the following areas:
  - Understand
  - Prevent
  - Detect
  - Respond
  - Recover
  - Improve

# Sampling of Workshop Themes

- Risk management accountability and responsibility needs to be clearly defined
- More work required to identify the unique privacy and civil liberties needs for critical infrastructures
- Different types of dependencies must be addressed: technology, business partner, and process
- There is a need to have cybersecurity trained workforce
- Modular model viewed as beneficial to identify and prioritize areas for potential investment, scales for wide range of enterprise sizes
- Foundational cybersecurity practices continues to be an identified gap

# Next Steps

In June 2013, we will post on the Framework website http://www.nist.gov/itl/cyberframework.cfm:

- A summary of this Workshop
- An illustrative outline of the Framework

# Stay Engaged

Please send us your notes, continued observations, and further suggestions at cyberframework@nist.gov;

Look again at the Analysis and Responses at http://www.nist.gov/itl/cyberframework.cfm;

Review and Comment on the Next Set Deliverables to be posted in June 2013;

**3rd Cybersecurity Framework Workshop**
**July 10-12 at the University of California San Diego**

Thank you Carnegie Mellon University for hosting the 2nd Cybersecurity Framework Workshop