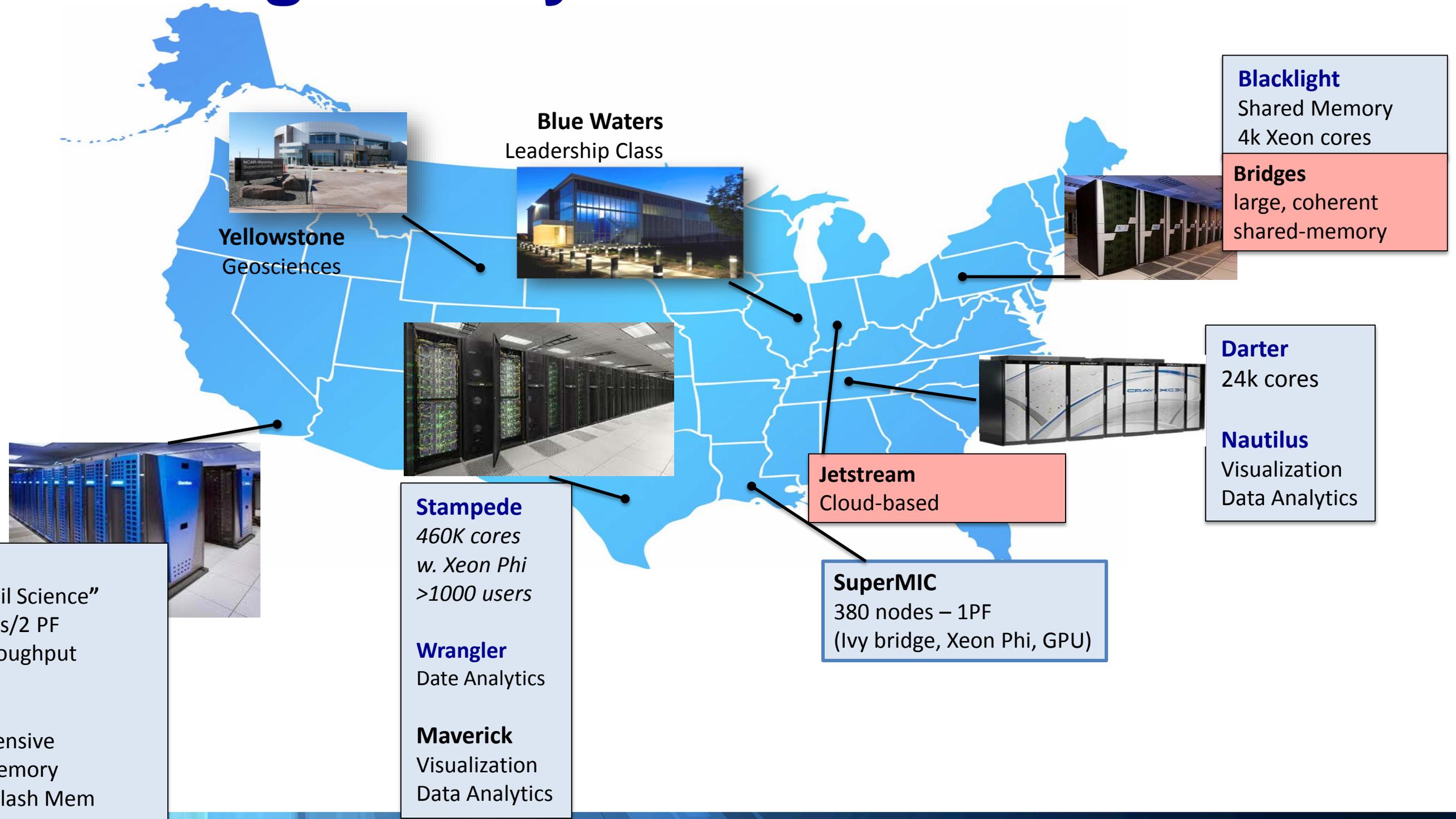


# HPC Security: NSF Perspective



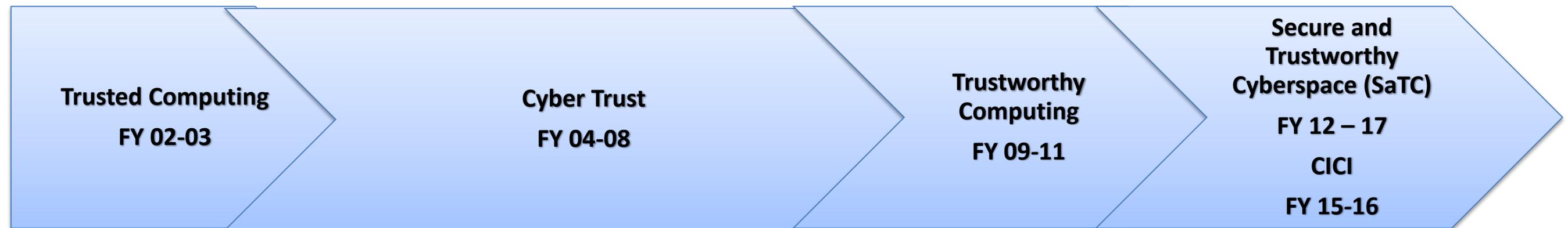
ANITA NIKOLICH  
CISE/ACI  
SEPTEMBER, 2016

# HPC: Long History of NSF Investments



# Security (and IDAM): Long History of NSF Investments in Basic and Applied Research

- 14 Years and \$800M+ of funding NSF security researchers



# HPC + Security: Areas of Opportunity for New Research

- Instrumentation/Tools for security. Traditional “enterprise security” approach inadequate.
- Data Integrity throughout the scientific lifecycle for large scale data sets
- Formal methods for integrated hardware/software security
- Introducing security into ENG work – ie new chipsets, optical, quantum



# HPC + Security: Areas of Opportunity for Operational Cyberinfrastructure

- Further increase security awareness among NSF-funded Large Facilities
- Foster a community around best practices and incident handling
- Security is mandated by Agreements but execution varies wildly. Standardize security plans.
- Data Management practices
- Identity and access management - secure, multi factor IAM and solid security group policies
- Scientific Software – security will become more fundamental

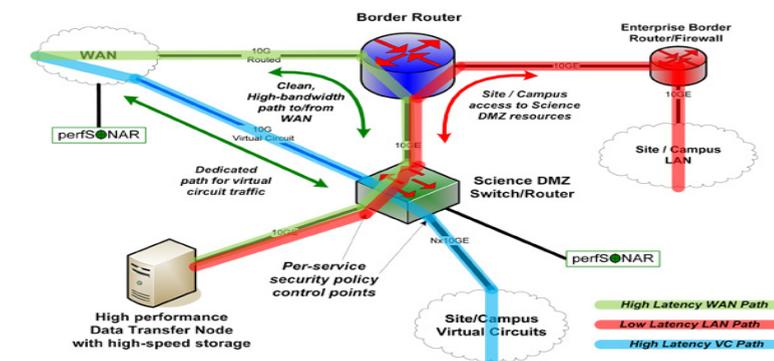


# HPC: Traditional Models are Changing

- Cloud – where will it fit in? How to ensure integrity and interoperability of on prem and commercial cloud
- Data will play a more central role considering the vast quantities that will be generated
- Our current end to end architecture (aka Science DMZ) not adequate
- Workforce development more important

**Simple Science DMZ Diagram**

A simple Science DMZ has several essential components. These include dedicated access to high-performance wide area networks and advanced services infrastructures, high-performance network equipment, and dedicated science resources such as Data Transfer Nodes. A notional diagram of a simple Science DMZ showing these components, along with data paths, is shown below:



The essential components and a simple architecture for a Science DMZ are shown in the Figure above. The Data Transfer Node (DTN) is connected directly to a high-performance Science DMZ switch or router, which is connected directly to the border router. The DTN's job is to efficiently and effectively move science data to and from remote sites and facilities, and everything in the Science DMZ is aimed at this goal. The security policy enforcement for the DTN is done using access control lists on the Science DMZ switch or router, not on a separate firewall.





***Thanks!***

