Cybersecurity Policy Briefing

Science Technology Telecommunications Committee

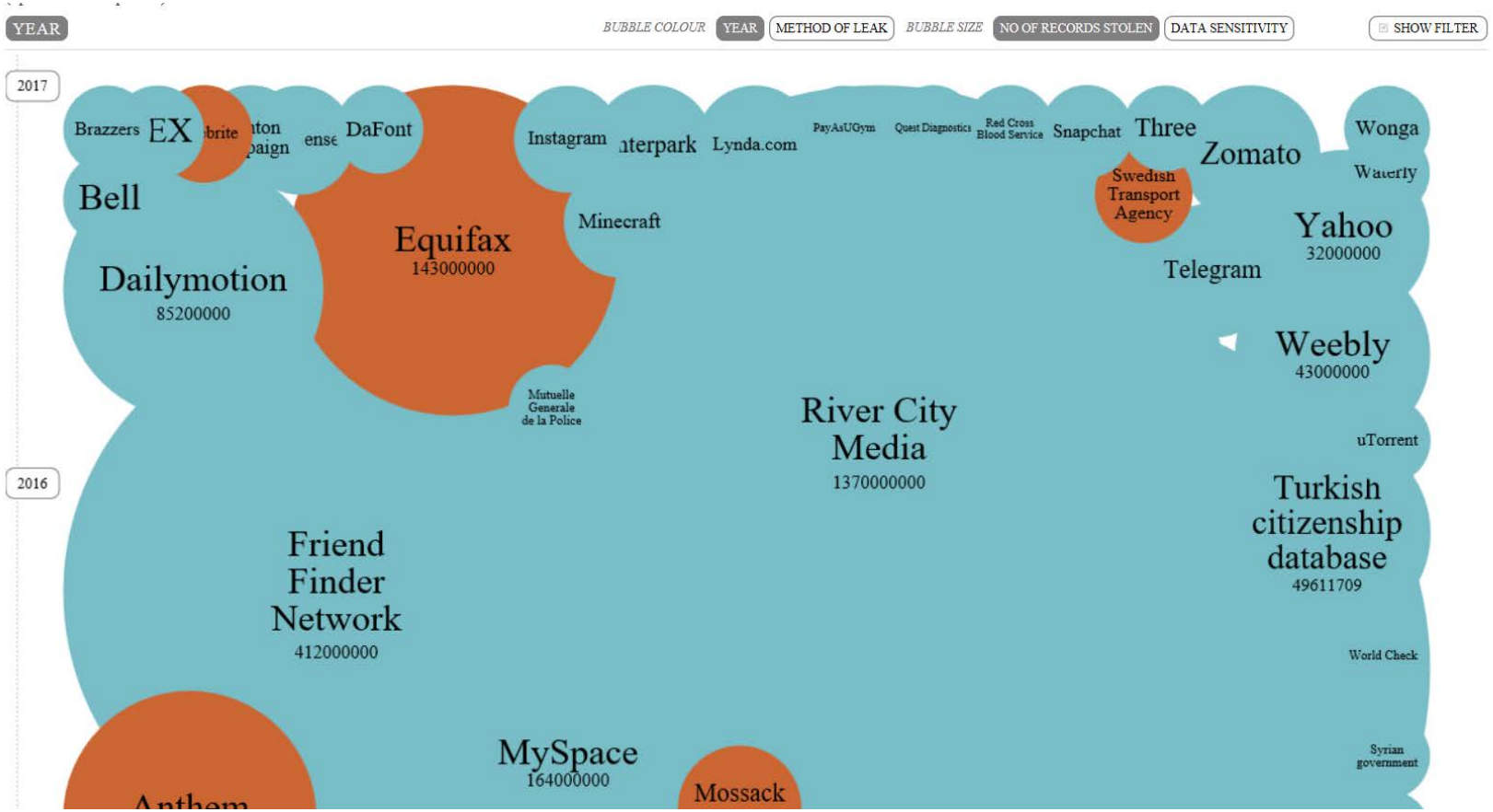
Katherine Martinez, Legislative Director, Century Link New Mexico

September 26, 2017

CenturyLink™

Data Breaches

Information is Beautiful website:



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

CenturyLink™

The Dynamic Cybersecurity Environment

- Cybercrime is a growth industry - the returns are great and the risks are low
  - Few of the biggest cybercriminals have been caught or, in many cases, even identified.

- Estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion… more than the national income of most countries and governments
  - Impacts of Cybercrime are difficult to estimate
  - Lack of Data
  - Intellectual Property difficult to value
    - Most important loss from cybercrime is in the theft of Intellectual Property (IP) and business confidential information, as this has the most significant economic implications.
    - Financial crime—the theft of financial assets through cyberintrusions—is the second largest source of direct loss from cybercrime.

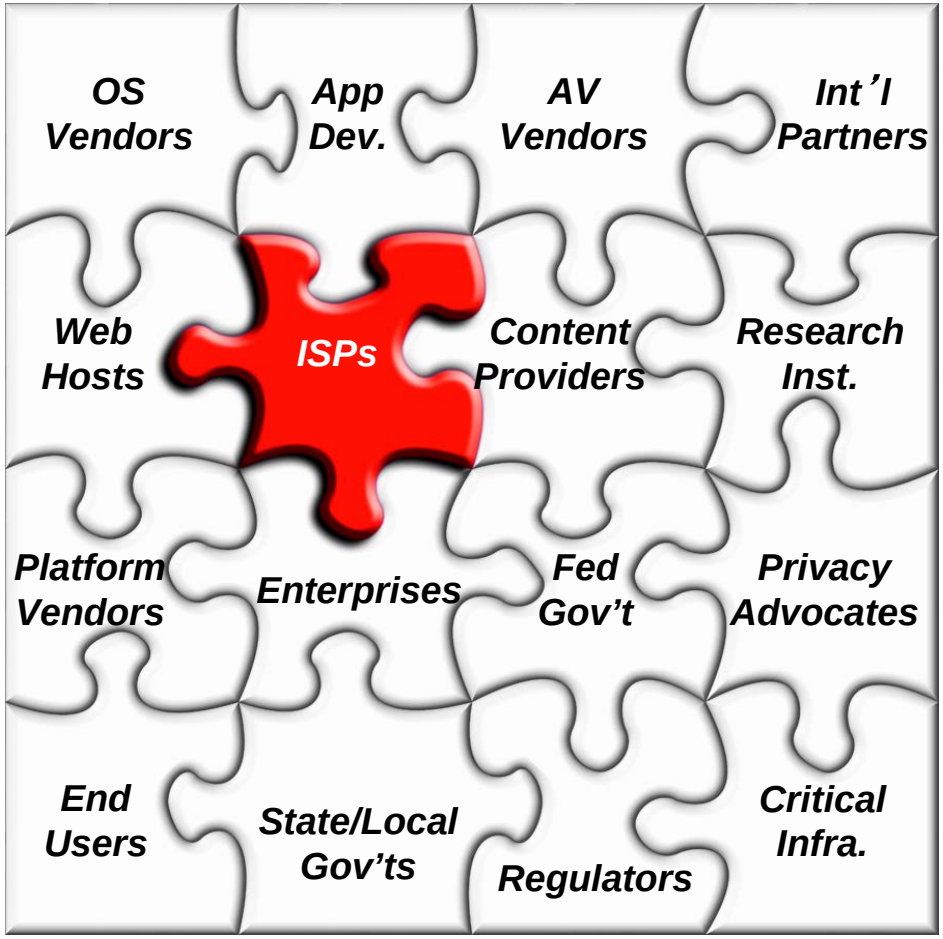
- Cyber-based attacks can have significant, and negative impacts to our company, our customers and to your state and citizens.

http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Cybersecurity Ecosystem-A Complex Environment

Cyber Ecosystem

- Comprises a variety of diverse participants – private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communications technologies) – that interact for multiple purposes.



CenturyLink & Cybersecurity

- Cybersecurity is one of CenturyLink's core competencies as we carry approximately 20% of the world's internet traffic on our networks

- To protect our customers, including commercial and government, we actively participate in numerous state, federal and industry forums and have established public/private partnerships with agencies such as DHS and DoD

- CenturyLink has more "information sharing" with US Government and Industry than virtually any other ISP
  - CenturyLink is deeply embedded within the oldest ISAC (Comm-ISAC) and within the DHS's National Cybersecurity and Communications Integration Center (NCCIC)

- The President's National Security Telecommunications Advisory Committee (NSTAC) has been asked to provide recommendations on ways to reduce the threat of botnet attacks.
  - The report will be provided in October. This stands to be an important industry reference.

- CenturyLink is actively engaged with state policy members: We are a corporate partner of the NGA Cybersecurity Policy Academy and participate on cyber matters in a number of state groups [e.g., NASCIO (state CIOs)] and legislative groups (e.g., NCSL, ALEC).
  - These groups and forums can help states understand and implement consistent cybersecurity best practices and recommendations for their administrative organizations and systems. As well, they work to promote the same practices for the state's resident and business ecosystem.

State & Local Level Concerns

- States provide critical services to, and hold information about, their citizens— which makes states a prime target for cybercrime
- States and local government are increasingly becoming a target of “hacktivists” who enter into systems for political or social motivations
- Cyber issues do not start/stop at the state borders
- Response to cyber events has to occur very quickly
- Disruptions can be significant and costly

Thoughts to Guide Your Approach to Cybersecurity

- *Dig your well before you are thirsty*: Cyber strategies are best developed in advance of any cyber event to ensure that mitigations and contingencies are in place.

- The NIST framework is helpful in guiding an approach to cybersecurity (see appendix)

- You should identify your "cyber partners" as part of state planning efforts, this should include not only governmental departments and agencies but private sector entities that provide essential services and/or have cyber expertise.

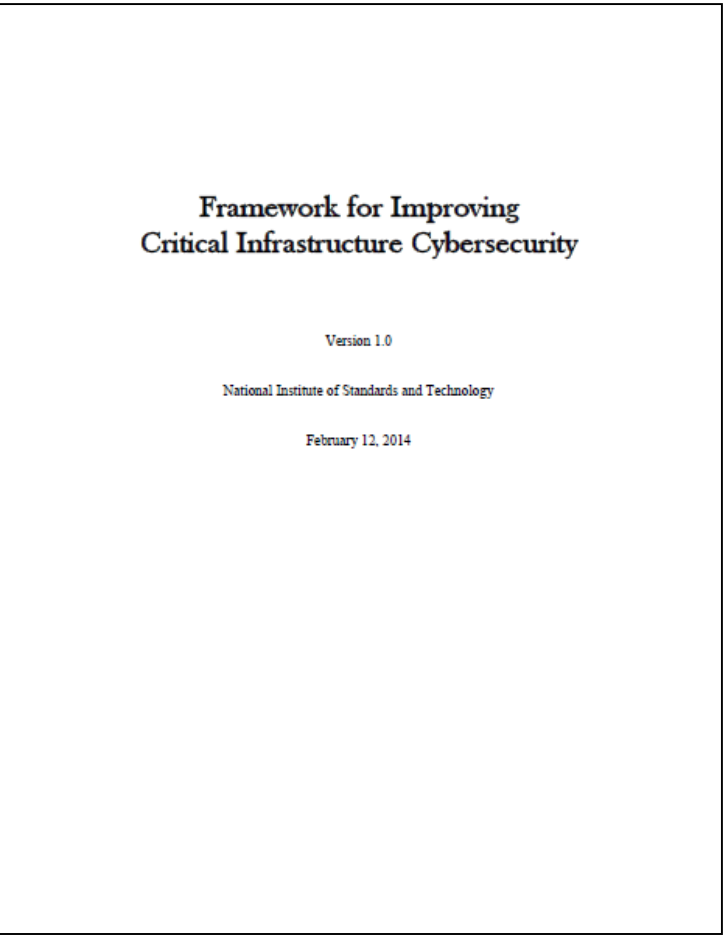
- Cyber coordination with industry should be coordinated through one Department/Agency and should be aligned with State Emergency Management Planning.

Thoughts to Guide Your Approach to Cybersecurity

- Cyber resiliency should be incorporated into state projects, programs and data/information assets.
- Consider the workforce and education needs of the state now and in the future for a cybersecurity workforce and include key educational entities in your planning/strategy.
- Dedicated funding for state cybersecurity efforts can provide resources to support your cybersecurity posture: planning, cyber-education, workforce development, testing and remediation.
- If your data is critical, it should be managed.

Appendix: NIST Cybersecurity Framework

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity**
  - Directed the Department of Commerce's - National Institute of Standards and Technology (NIST) to lead the development of a framework of cybersecurity practices to reduce cyber risks to critical infrastructure

- Cybersecurity risk is a reality that organizations must understand and manage like other business risks that can have critical impacts.

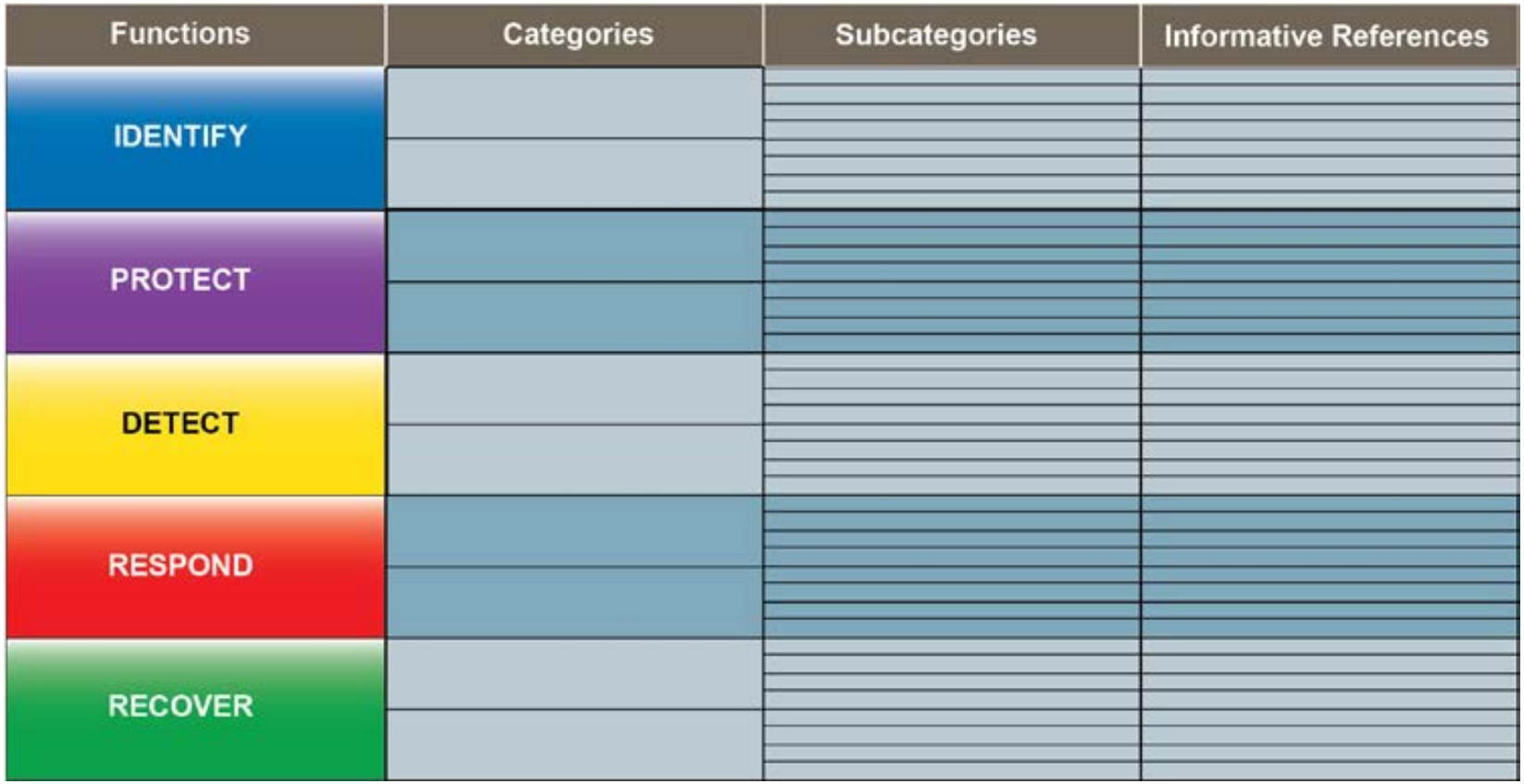
- Organizations must manage cybersecurity risk in order to gain and maintain customers, reduce cost, increase revenue, and innovate.

- The Framework is intended to help each organization manage cybersecurity risks while maintaining flexibility and the ability to meet business needs.

- Implementing the Framework will help organizations align and communicate their cybersecurity risk posture with their partners and help communicate expectations for managing cybersecurity risk consistent with their business needs.

CenturyLink™

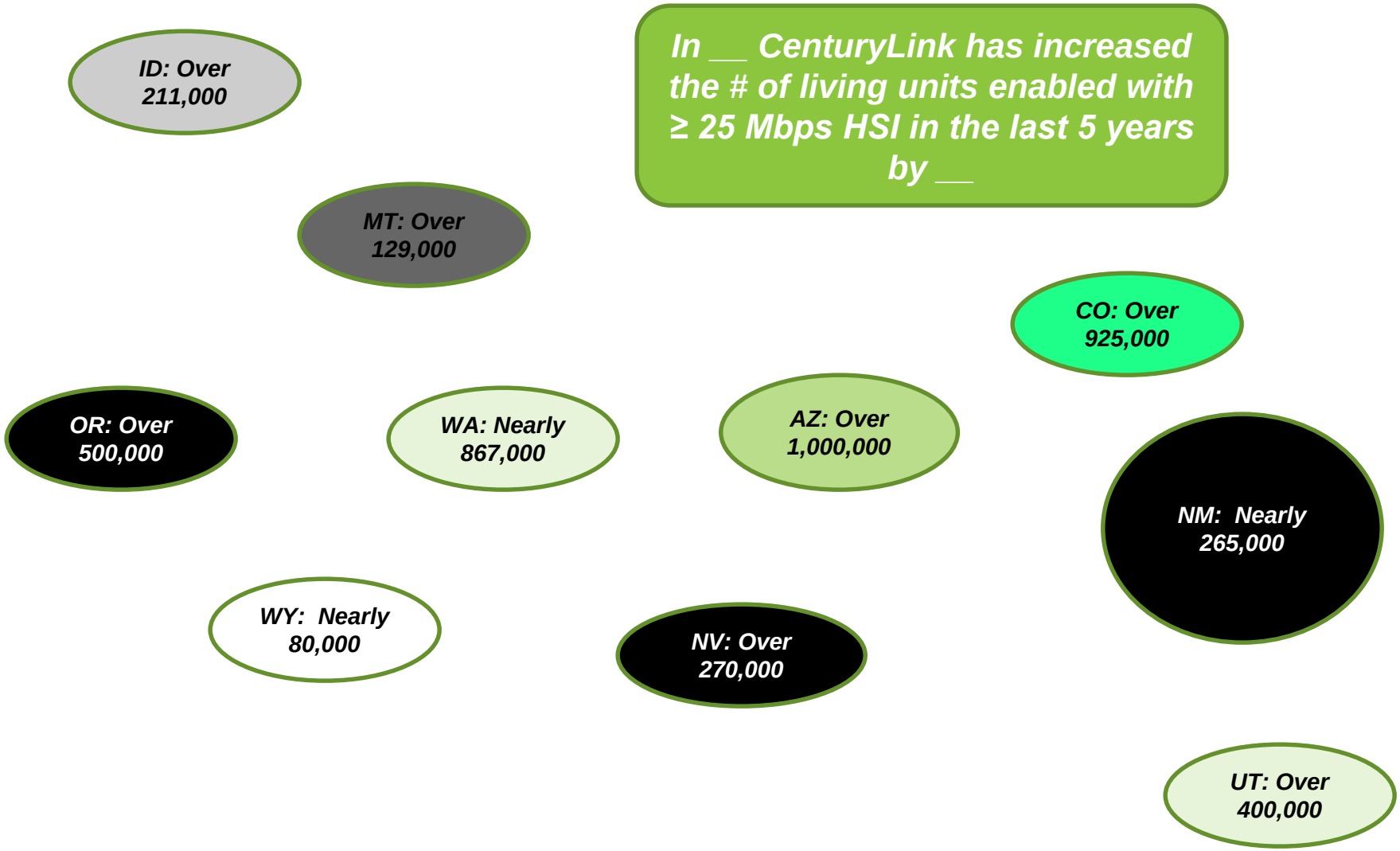
Appendix: NIST Cybersecurity Framework



Examples of Categories include "Asset Management," "Access Control," and "Detection Processes." Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."

CenturyLink™

Fill in the blank: Broadband Success Story: 2011 - 2016



CenturyLink™

State Broadband Grant Programs: Overview

CenturyLink has participated in Grant programs in 5 states in 2017

- Colorado, Minnesota, Nebraska, Wisconsin, Virginia
- New opportunities in **NM**, TN, and UT to be implemented in 2018
- New Mexico SB308 (Sen. Padilla) conversion of the NM USF to 5M (minimum) broadband fund
  - Underserved and unserved areas
  - Speed requirements
  - Matching funds
  - PRC still rule making

Common Characteristics

- Funding for projects in unserved and underserved areas
- Some level of matching funds required
- Defined build out periods and reporting; speeds required vary
- Open to competitors and challenges allowed

CenturyLink™