SAND2016-11692C

Exceptional service in the national interest

Sandia National Laboratories

Era of Cyber Solutions:

End User Cybersecurity

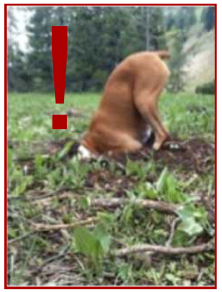
C. M. Keliiaa

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Cyber Basics

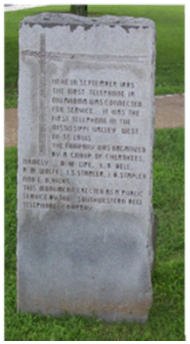
- Passwords
  - Do not share passwords & Change them when needed
  - Do not leave passwords in easy to find places (under the keyboard)
  - Use a passphrase to remember passwords (mDn1fK@cF$M)
- Email
  - Malicious Links – Install malicious software
    - Roll over to review without clicking!
  - Phishing & Speer Phishing – Might Look Official, but…
    - Is anything amiss? Misspellings? Out of the ordinary?

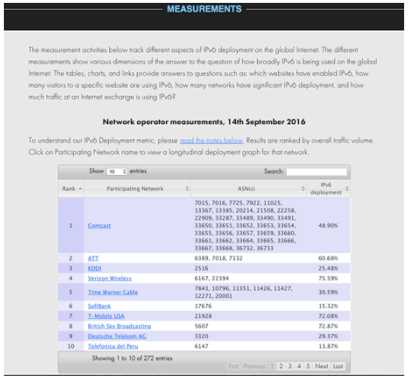


- Social Engineering
  - Do not disclose passwords or act on the behalf of an unsolicited call
    - No matter how convincing they seem – Say you'll verify & call back
- Social Networking
  - Do not post anything you wouldn't want your Grandma to see
  - Be Smart – Know Who Your Friends Are, Be Safe – Known Web Sites

Not Just Computers Anymore

- Mobility
  - Internet Access Wherever You Go – Maybe?
  - Radio + Internet – Super Computer in Your Pocket!
  - Malicious Smart Phone Apps Too!
- Cloud
  - Data Stewardship – Read the Fine Print
  - Are They Going to Protect Your Data or Take It?
- What is the Internet of Things?
  - More than the refrigerator
  - Smart Energy
  - Telemedicine
  - Mobile Networks





http://www.worldipv6launch.org/measurements/

End User Cybersecurity@Work

Sandia National Laboratories

- Accountability, Policies, & Guidelines
  - Appropriate Use, Waste, Fraud & Abuse Policies
  - Human Resource Employee Manuals
  - Training, Education, & Awareness

- Records Management
  - A “Record” is any recorded information made or received in the course of business or government operations
  - Records Retention & Disposition – Office of Official Records
- Information Categorization, Value, & Protection
  - Public, Sensitive, Proprietary, Statutory, Privileged, Personal
  - Value to You & Others
  - Unauthorized Access, Modification, Destruction, Disclosure, Loss of Information

* You are the first and last Line of defense!

Cyber Risk: What to Do?

- Spam – Unsolicited Emails – Annoying & Bad
  - Get to Know Your Cybersecurity Response Team
  - Forward Suspicious Emails to Cybersecurity for Review First
- Data Ownership & Data Stewardship
  - Ownership - Intellectual Capital, Copyrights, Trademarks, Patents
  - Stewardship - Data Management, Storage, & Sharing
- Data In-Transit, At-Rest, & In-Process
  - Data protection in all cases
- Risk Management
  - Physical Assets
  - Cyber Assets
- Privileged Accounts vs User Accounts
  - Separate Privileged Access From User Access

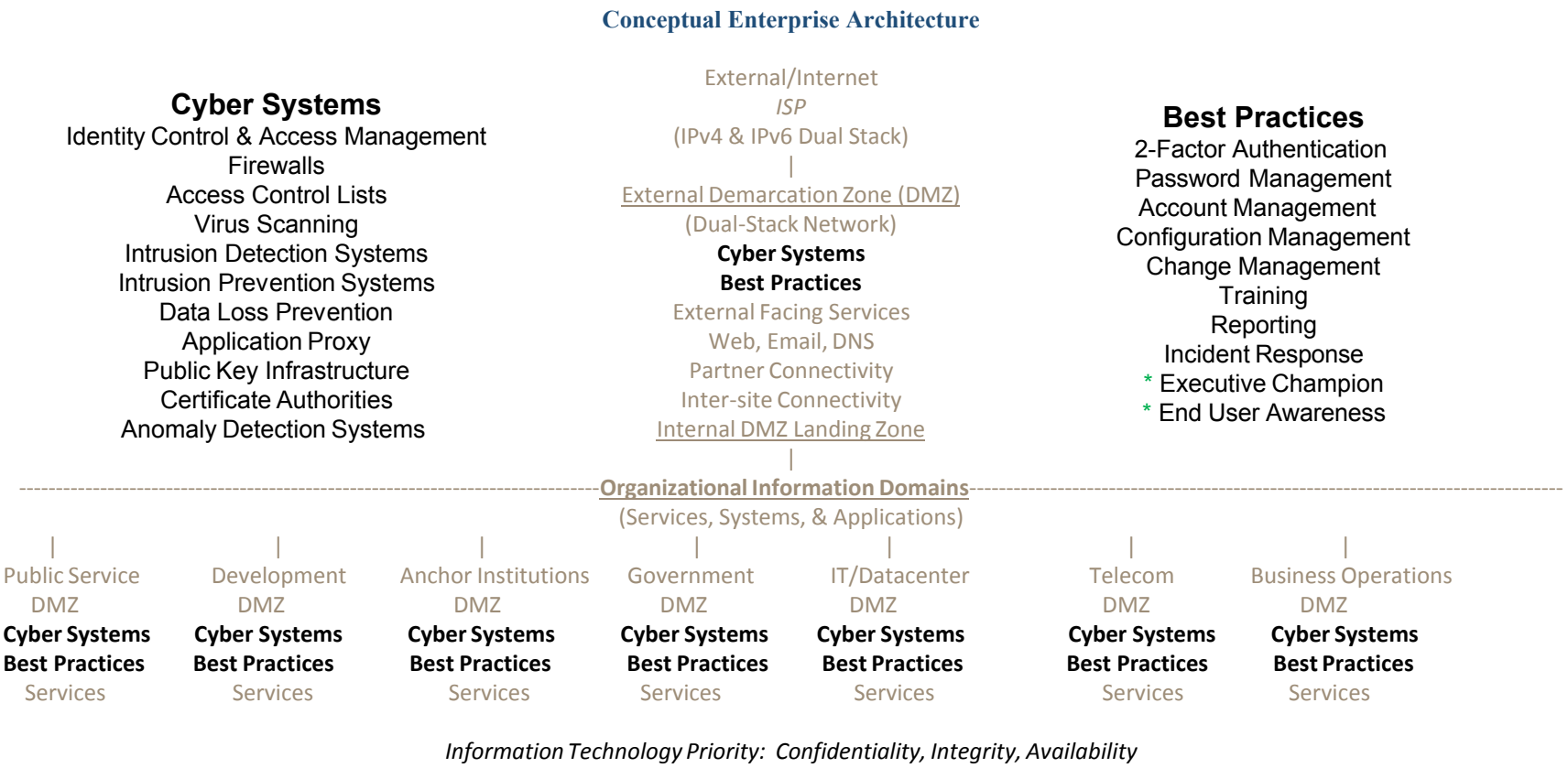
Core

Cybersecurity Framework Component

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

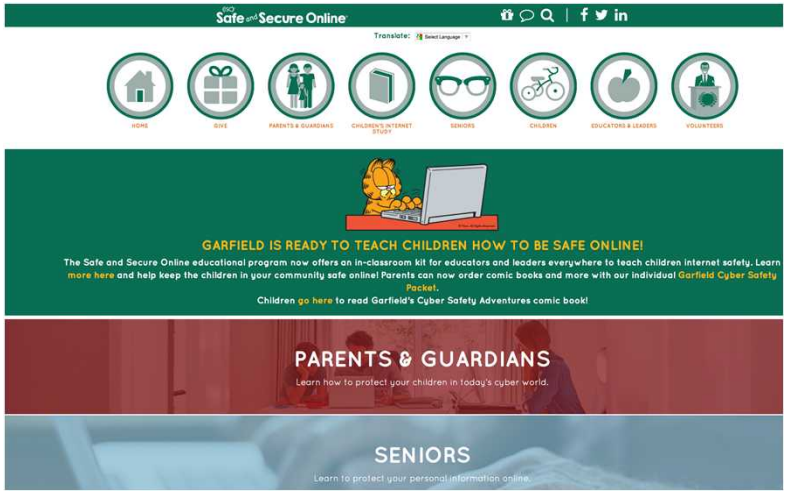
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Behind The Scenes



* You are the most important part of protection!

Best Practices



https://safeandsecureonline.org

https://www.isc2.org

https://www.sans.org

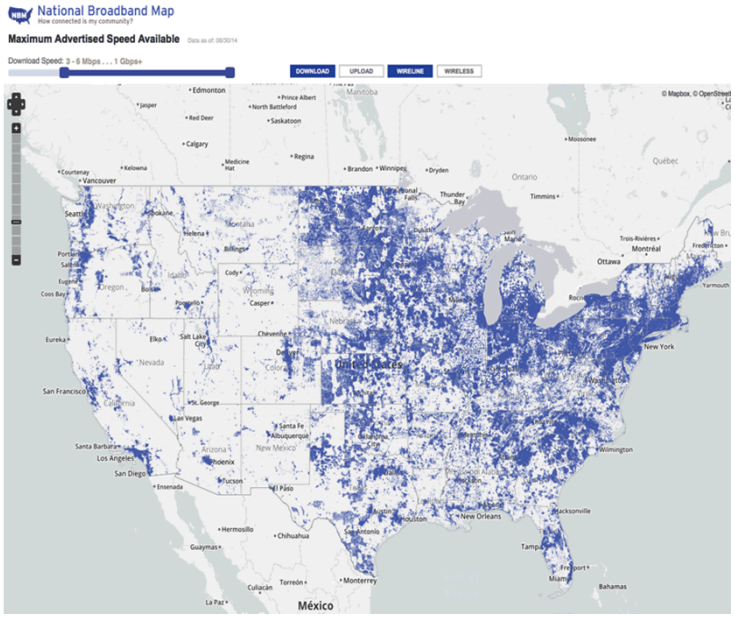
CIS Critical Security Controls - Version 6.0

To learn more about the CIS Critical Security Controls and download a free detailed version please visit:
http://www.cisecurity.org/critical-controls/

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewall Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises

The Tribal Digital Divide

Source: https://www.census.gov/geo/maps-data/maps/aian_wall_maps.html



Source: http://www.broadbandmap.gov/speed

Internet Past, Present, & Future

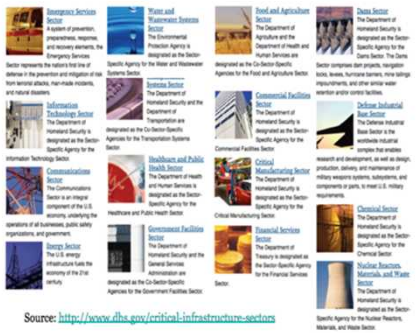
Sandia National Laboratories

Sandia National Laboratories

Tribal Cyber Infrastructure Assurance Initiative

Sandia Labs Collaboration

- Government to Government
- National Security
- Objective Advisory
- Does Not Compete With Industry
- Cyber Critical Infrastructure Modernization



Department of Homeland Security Critical Infrastructure Sectors

Cyber	Science & Engineering Based Cyber Interdisciplinary Expertise
	Secure Cyber Infrastructure Modernization – Information & communication technologies (ICT) Radio frequency (RF) and Internet protocol (IP) modernization assessment with cyber security path forward for emergent information services.
	Risk Management – Assessment of technical risks, business continuity, and risk involving quantitative/probabilistic and qualitative/difficulty-of-attack risks and mitigation recommendations.
	Adversary-Based Security – Assessment of adversarial threat to organizational processes and technical infrastructure with mitigation recommendations to increase protection against adversarial cyber attack for customer organizations.
Resilience	**Resilient Infrastructure Systems** – Infrastructure disruption consequence and dependency analysis to include critical infrastructure security and resiliency recommendations. Ensures resilience of infrastructure services to disruptive events for customer critical infrastructure services.
	Trusted and Secure Systems – Provides methods and tools for mitigating vulnerabilities, often identified by other analysis and assessment methods, and for ensuring delivered systems fail secure during service degradation or disruption.
Human	**Cyber Centric Training, Exercise, and Analysis** – Integrated incident response, forensics, and human element exercises with interactive customer leader-led and/or online training to increase cybersecurity knowledge for decision makers and operators.
Architecture & Design	**Technical Assistance** – Energy efficiency, facilities, and information service technical assistance with architecture/design/build guidance to enhance development of emergent next generation services tailored to customer needs.
Engineering	**Cyber Safeguard Engineering** - Science and engineering based cyber (S&EC) safeguard and countermeasure tech transfer. Federally funded research and development center (FFRDC) risk mitigation to changing ICT challenges. Mutual Benefit: S&EC Assurance/Tech Transfer
R&D	**Cyberspace Research and Development** – Tribal single-point of authority partnership to yield National level Cyber solutions. High performance computing analysis of national priority problems and modeling and simulation, are areas of opportunity. Our vision is collaboration via a subset of complex infrastructure and scope of a sovereign government's needs and requirements. Mutual Benefit: Shared Cyberspace Solutions

Questions and Discussion

Sandia National Laboratories

Era of Cyber Solutions

End User Cybersecurity

THANK YOU!

Curtis Keliiaa

CISSP/IPv6 Forum Gold Certified Engineer

Sandia National Laboratories

(505) 845-0185

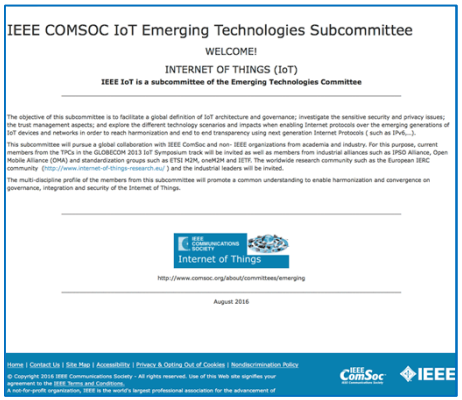
cmkelii@sandia.gov

Supplemental Slides

Sandia National Laboratories

A Bit Technical

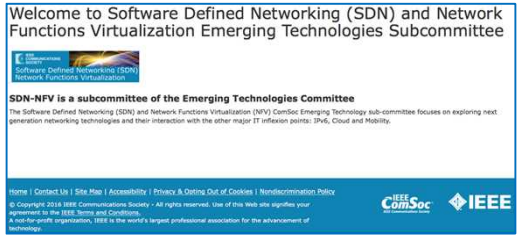
Next Generation Happening Now



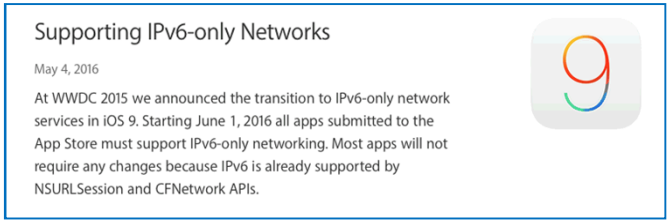
Source: http://iot.committees.comsoc.org

Source: http://ti.committees.comsoc.org

Source: http://5gmwi.committees.comsoc.org



Source: http://sdnnfv.committees.comsoc.org



Source: https://developer.apple.com/news/?id=05042016a

Cybersecurity Design Requirement

Sandia National Laboratories

Conceptual IPv6 Security Reference Architectures