

Exceptional service in the national interest



Cyber and Infrastructure Security



Era of Cyber Solutions: End User Cybersecurity



C. M. Keliiaa

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

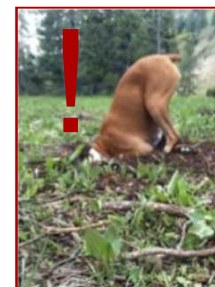
Cyber Basics

■ 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 & Spear Phishing – Might Look Official, but...
 - Is anything amiss? Misspellings? Out of the ordinary?



■ Social Engineering

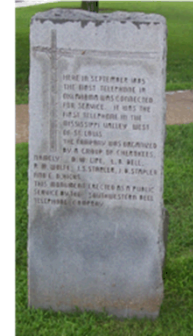
- Do not disclose passwords or act on the behalf of an unsolicited call
 - No matter how convincing they seem – Say you'll verify & call back

■ 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



MEASUREMENTS

The measurement activities below track different aspects of IPv6 deployment on the global Internet. The different measurements show various dimensions of the answer to the question of how broadly IPv6 is being used on the global Internet. The tables, charts, and links provide answers to questions such as: which websites have enabled IPv6, how many visitors to a specific website are using IPv6, how many networks have significant IPv6 deployment, and how much traffic at an Internet exchange is using IPv6?

Network operator measurements, 14th September 2016

To understand our IPv6 Deployment metric, please [read the notes below](#). Results are ranked by overall traffic volume. Click on Participating Network name to view a longitudinal deployment graph for that network.

Rank	Participating Network	ASN(s)	IPv6 deployment
1	Comcast	7015, 7016, 7725, 7922, 13021, 13103, 13160, 20124, 21506, 22258, 22909, 32147, 33449, 33490, 33491, 33605, 33651, 33652, 33653, 33654, 33655, 33656, 33657, 33658, 33660, 33661, 33662, 33664, 33665, 33666, 33667, 33668, 36732, 36733	44.90%
2	AT&T	6199, 7014, 7121	60.68%
3	ISDCE	2536	25.48%
4	Verizon Wireless	6167, 21794	75.59%
5	Telia Norway Cable	7841, 10798, 11331, 11406, 11427	35.59%
6	SoftBank	12279, 20091	15.32%
7	E-Stream Ltd	21924	72.08%
8	World Site Broadcasting	1667	72.07%
9	Deutsche Telekom AG	3320	29.37%
10	Telefonica del Peru	6147	13.87%

Showing 1 to 10 of 272 entries

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

End User Cybersecurity@Work

- 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

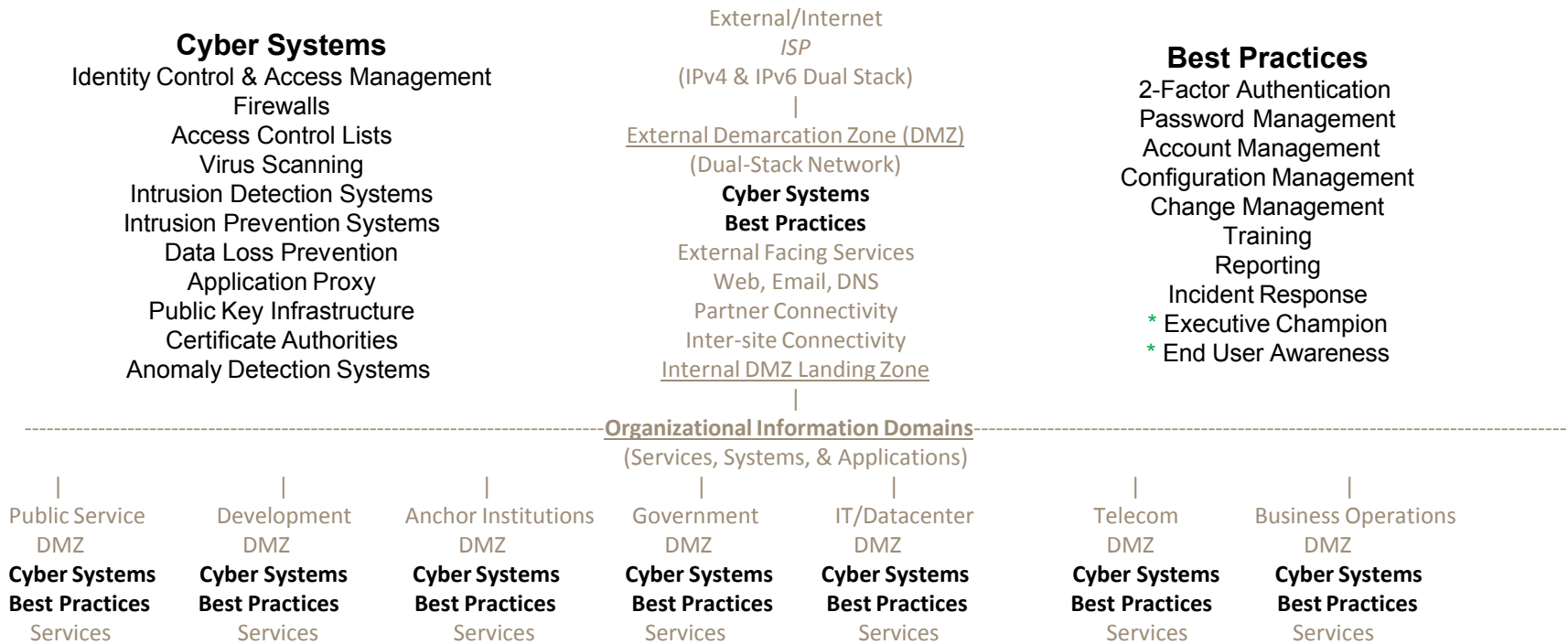
Core
Cybersecurity Framework Component

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
Detect	Maintenance	PR.MA
	Protective Technology	PR.PT
	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
Respond	Detection Processes	DE.DP
	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
Recover	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements Communications	RC.IM

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

Behind The Scenes

Conceptual Enterprise Architecture



Information Technology Priority: Confidentiality, Integrity, Availability

* You are the most important part of protection!

Best Practices



Safe and Secure Online

Translate:

HOME | SAVE | PARENTS & GUARDIANS | CHILDREN'S INTERNET STUDY | SENIORS | CHILDREN | EDUCATORS & LEADERS | VOLUNTEERS

GARFIELD IS READY TO TEACH CHILDREN HOW TO BE SAFE ONLINE!

The Safe and Secure Online educational program now offers an in-classroom kit for educators and leaders everywhere to teach children internet safety. Learn [more here](#) and help keep the children in your community safe online! Parents can now order comic books and more with our individual **Garfield Cyber Safety** (packet).

Children go [here](#) to read Garfield's Cyber Safety Adventures comic book!

PARENTS & GUARDIANS
Learn how to protect your children in today's cyber world.

SENIORS
Learn to protect your personal information online.

<https://safeandsecureonline.org>



ISC2 IMPROVING A SAFE AND SECURE CYBER WORLD

Home | Certifications | Associate of ISC2 | Training | Events | Special Programs | Members Only | About | Contact Us

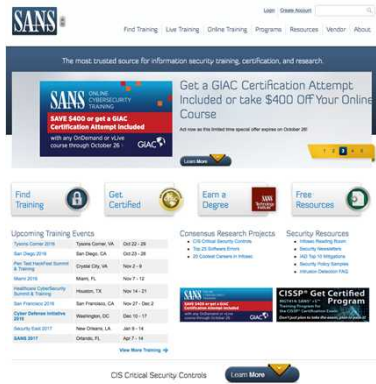
TRANSFORM THE FUTURE 11th Annual Cyber Security Conference

Industry-Leading Cybersecurity Certifications

- SCSCP**: Information Management and support the central security control objectives of...
- CCSP**: Cloud Security: Physical, security, and management aspects of cloud computing...
- CCSP**: Leadership & Governance: Design, develop, and manage the most security critical...

World-Class Cybersecurity Training

<https://www.isc2.org>



SANS The most trusted source for information security training, certification, and research.

Get a GIAC Certification Attempt Included or take \$400 OFF Your Online Course

Find Training | Live Training | Online Training | Programs | Resources | Vendor | About

Upcoming Training Events

Systems Center 2016	Tampa, GA	Oct 22 - 28
San Diego 2016	San Diego, CA	Oct 23 - 29
Cloud Security Summit & Training	Cloud City, VA	Nov 1 - 3
Heaven 2016	Heaven, UT	Nov 7 - 12
Hardware CyberSecurity Summit & Training	Houston, TX	Nov 14 - 21
San Francisco 2016	San Francisco, CA	Nov 21 - Dec 2
Cloud Security Summit 2016	Birmingham, AL	Dec 10 - 17
Heaven Cyber 2017	Heaven, UT	Jan 8 - 14
SANS 2017	Orlando, FL	Apr 7 - 14

Consensus Research Projects

- CIS Critical Security Controls
- Top 20 Software Errors
- 20 Critical CVEs in History

Security Resources

- Virtual Patching Exam
- Security Readiness
- Top 100 Insights
- Monthly Patch Statistics
- InfoSec Decision Matrix

CISSP® Get Certified Program

<https://www.sans.org>

<https://www.sans.org>

CIS Critical Security Controls - Version 6.0

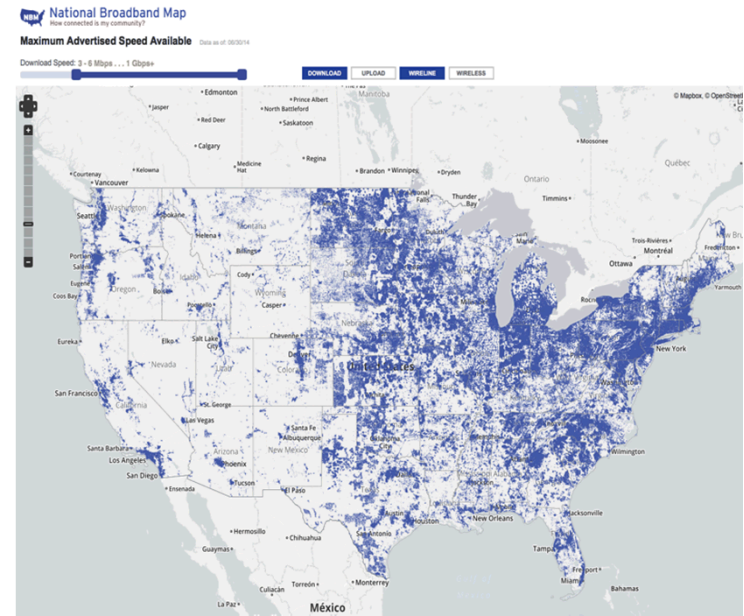
To learn more about the CIS Critical Security Controls and download a free detailed version please visit: <http://www.cisecurity.org/critical-controls/>

- 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



We're Going to Need A Bigger Boat!

- ICT Modernization Sea Change
(Mobile Networks/IOT/Big Data)
- Critical Infrastructure Modernization
(ICT-ICS-SCADA Integration)
- Cybersecurity Design Requirement
- Workforce Development
- Minimize Complexity, Risk, & Cost
- ROI - Internet Continuity



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

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

A Bit Technical

Cybersecurity Design Requirement

Conceptual IPv6 Security Reference Architectures

