SAND2016-11059C

Data Governance: ICT Modernization Impacts to Business Operations

Abstract

The internet protocol (IP), version 6 (IPv6) provides necessary address space for ongoing internet innovation. The American Registry for Internet Numbers (ARIN) IPv4 free pool was exhausted on 9/24/2015, subsequently the Internet Engineering Task Force (IETF) obsoleted the IPv4 standards on 3/14/2016. IPv6 deployment is inevitable to sustain continuity of information services. Concerns are increased complexity, risks, and operational costs because IPv4 and IPv6 are not interoperable. Data-governance is discussed with regard to information and communication technologies (ICT) modernization, business continuity, risk management, and mobile and enterprise impacts.

ICT Modernization

IPv6 adoption has been slow because IPv4's predominance has delayed the roll out for IPv6, until now…

1. Dual-Stack
   a. Risk*: If ICT infrastructure is dual-stack enabled then technical complexity, cybersecurity risks, and operational costs increase*
   b. Mitigation: *Maximize return on technical investments by reducing complexity, risks, and costs*
2. Protection Posture
   a. Risk: *If IPv4 and IPv6 do not have a balanced and equivalent protection posture for common information assets then a latent threat exists which increases the likelihood of adversarial success of compromise if attacked*
   b. Mitigation: *Use of a cyber-centric approach with cybersecurity as a design requirement for information assets and cybersecurity regimes utilizing IPv4 and IPv6 to identify and implement appropriate protection mechanisms*

A little Internet history

One Information Super Highway – IPv4 Born 1981, standardized 1983, WWW 1991 (25-year anniversary), RIP 2015

Internet: Single-Stack
Systems: IPv4 Single-Stack
Networks: IPv4 Single-Stack
IPv4 is exhausted and obsoleted

Where is everyone going?

Two Information Super Highways – IPv6 Born 1999, Graduation – NOW!
IPv4 and IPv6 are distinctly different and vastly different in scale

Internet: Dual-Stack IPv4 & IPv6
Systems: Dual-Stack IPv4 & IPv6
Mobility: Dual-Stack IPv4 & IPv6
Cloud: Dual-Stack IPv4 & IPv6
Networks: Dual-Stack IPv4 & IPv6
Dual-Stack adds increased complexity, risks, and costs by adding an additional attack surface
A latent threat exists if the two protocols do not have a balanced protection posture for dual-stack information assets

What about IPv6 only?

Digital Divide and a New Super Highway

Internet: Single-Stack
Systems: IPv6 Single-Stack
Mobility: IPv6 Single-Stack
Internet of Things: IPv6 Single-Stack
Cloud: IPv6 Single-Stack
Networks: Dual-Stack IPv4 and IPv6
(Why would the network need to be dual-stacked?)
Single-Stack IPv6 reduces complexity, risk, and costs by removing IPv4 dependencies
When IPv6 market penetration is sufficient, IPv6 predominance will accelerate IPv4's decline

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.

Data Governance: ICT Modernization Impacts to Business Operations

IPv4 to IPv6 Transition Mechanisms

Native IPv6 operation is preferred to minimize cost associated with dependencies that are hard to disposition

Dual-Stack
Tunneling
Application Layer Gateways
Network Address Translation

NAT and Automated Tunneling (Protocol 41) add complexity, risk, and cost
Dual stack provides dual functionality but not interoperability
ALG's and tunneling should be implemented by design requirement not just transition

IP Version Differences

Property	**IPv4**	**IPv6**
Address, Network Size	32 bits, 8-30 bits	128 bits, 64 bits
Notation	Dot-delimited "." decimal	Colon-delimited ":" hexadecimal
Packet Header Size	20-60 bytes	40 bytes
Header-level Extension	Limited number of small IP options	Unlimited number of extension headers
Fragmentation	Sender or any intermediate router	Sender only
Control Protocols	ARP[1], ICMP[2], other protocols	NDP[3], ICMPv6
Minimum MTU[4]	576 bytes	1280 bytes
Path MTU discovery	Optional	Strongly recommended
Address assignment	One address per host	Multiple addresses per interface
Address types	Unicast, multicast, broadcast	Unicast, multicast, anycast
Subnet/Vlan[5] Identifiers	One subnet/VLAN ID per interface	Multiple subnet/VLAN ID's per interface
Address configuration	Manually, DHCP[6]	SLAAC[7], DHCPv6, Manual, Mobile IP (MIPv6)

IPv4 32-bit Address Example

Total IPv4 32 Bit Address Space 4.3 Billion – NO VACANCY

8 Bit Network Prefix	24 Bit 16 Million Hosts	10.0.0.0 Class A
16 Bit Network Prefix	16 Bit 65 Thousand Hosts	10.10.0.0 Class B
24 Bit Network Prefix	8 Bits 255 Hosts	10.10.10.0 Class C
/8-30 CIDR-VLSM Network Prefix	24 – 2 Bit Hosts	10.10.10.0/24

IPv6 128-bit Addresses

Total IPv6 128 Bit Address Space $3.4*10^{38}$ (Trillion, Trillion, Trillion)

2001:DB8:ABCD:EF0F:0123:4567:89AB:CDEF/128

"*/32*" Global Routing Prefix:	"*/64*" Network Prefix	"*/128*" when the 64 bit Host ID is added

Key Points:

1. IPv4 cannot accommodate growth, such as in cloud computing, mobility, and the Internet of Things (IoT)
2. IPv4 and IPv6 are distinctly different in function - Knowing IPv4 doesn't mean you know IPv6
3. IPv4 (4.3 Billion) and IPv6 (Trillion, Trillion, Trillion) are vastly different in scale
4. Modern network and systems gear comes IPv6 capable (circa 2010)
5. Security and cloud products may lack sufficient IPv6 capability
6. New workforce knowledge, skills, and abilities (KSA) are required to engineer, secure, and maintain IPv6 networks

[1] Address Resolution Protocol
[2] Internet Message Control Protocol
[3] Neighbor Discovery Protocol
[4] Maximum transmission unit
[5] Virtual local area network
[6] Dynamic Host Configuration Protocol
[7] Stateless Address Auto-configuration

Data Governance: ICT Modernization Impacts to Business Operations

Data Governance

Data Governance considerations are generally technology independent.

1. Policy & Data Handling
    a. Risk: *If appropriate use policies are not in place then the risk that waste, fraud, and abuse of information assets occur unabated is increased*
    b. Mitigation: *Implement, enforce, and socialize legally reviewed and approved appropriate use policy (log-on banners, training, and reporting) for the protection of sensitive and personally identifiable information (PII)*
2. Big Data
    a. Risk: *If knowledgeable use of information at scale is insufficient then the risk that important information is missed resulting in failure to recognize key issues is increased*
    b. Mitigation: *Implement assessment, analysis, and tools (data analytics) to increase data comprehension and knowledgeable use of information in a timely manner*
3. Data Categorization & Protection
    a. Risk: *If data is not appropriately categorized (valued) and protected (at rest, in motion, and in processing) in compliance with designated approving authorities then the risk of release of sensitive information with damaging consequences is increased*
    b. Mitigation: *Data categorization and implementation of standard and industry best practice protection mechanisms*
4. Partnerships & Collaboration
    a. Risk: *If partnership and collaborative data ownership and stewardship policies and protection mechanisms are not established such that data is protected across jurisdictions then the risk of exploitation of trusted relationships and operations is increased*
    b. Mitigation: *Collaborative service level agreements, non-disclosure agreements, incident response plans, and implementation of common or industry best practices, process and procedures*

Business Continuity Planning

Business continuity include emergency management, continuity of operations and IT disaster recovery concerns

1. Resilience of Critical Infrastructure
    a. Risk: *If the capability to survive impactful events is lacking then the risk of catastrophic organizational or system failure is increased*
    b. Mitigation: *Identify critical operations and process dependencies and implement contingency plans*
2. Emergency Management
    a. Risk: *If critical information is insufficient or communications are insufficient or inoperable during crisis then the risk of failed emergency response is increased*
    b. Mitigation: *Identify organizational and technical interoperability dependencies such as communications and conduct stakeholder and practitioner tabletop exercises*
3. IT Disaster Recovery
    a. Risk: *If information and associated information infrastructure including information asset recovery capabilities are insufficient to continue or resume critical operations then the risk of catastrophic organizational or system failure is increased*
    b. Mitigation: *Backups, hot, warm, cold alternate sites, cloud, and prioritization of services*
4. Continuity of Government (COG) & Continuity of Operations Planning (COOP)
    a. Risk: *If government and/or critical organizational operations are inoperable during time of crisis then the risk of catastrophic organizational failure is increased*
    b. Mitigation: *Identify critical services and personnel, and implement contingency and continuity plans*
5. Knowledge, Skills, & Abilities
    a. Risk: *If knowledge to design, secure, and operate information infrastructure with over dependence on IPv4 and not IPv6 ICT then the risk of gradual disconnection from internet resources utilizing IPv6 ICT is increased*
    b. Mitigation: *Training and executive championship to enable the workforce to implement IPv6 ICT*
6. Interoperability
    a. Risk: *If technical, syntactical, semantic, and organizational interoperability are insufficient then the risk of failed interjurisdictional communications and joint response to crisis is increased*
    b. Mitigation: *Stakeholder and practitioner tabletop exercises, training for personnel*

Data Governance: ICT Modernization Impacts to Business Operations

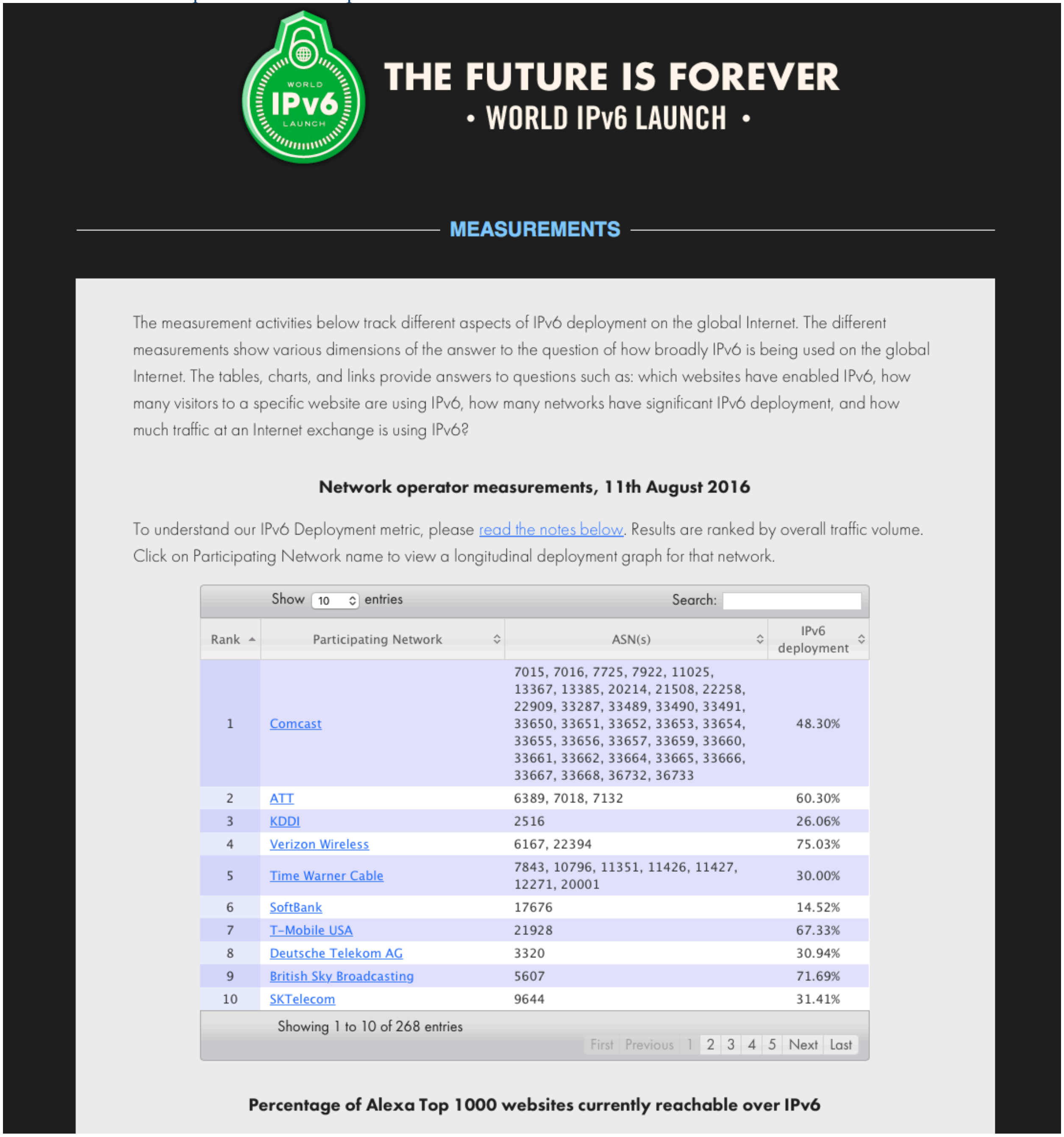
Risk Management

1. Threat Exposure
    c. Risk: *If threat exposure is such that an adversary has means, motive, and opportunity then the risk of compromise of information assets is increased*
    d. Mitigation: *Physical, personnel and cybersecurity assurance with adversary-based security assessment to identify and mitigate vulnerabilities including quantitative (value vs. cost) and qualitative (difficulty of attack) risk management, and cybersecurity and safety training and education for professionals, communities, and families.*
5. Cybersecurity
    a. Risk: *If dual-stack cyber protection posture is insufficient then the risk of compromise of information assets via IPv4 or IPv6 latent threat is increased*
    b. Mitigation: *Identify, implement, and manage protection mechanisms for IPv4 and IPv6 dual-stack, including adjacent (partner networks) and operational (i.e. social engineering) attack surfaces*
6. Authorization, Authentication & Accounting
    a. Risk: *If accountability, appropriate authority to conduct work, and authentication protection mechanisms are insufficient then the risk of unauthorized access and inappropriate or malicious activities is increased. Secondarily, if authorization, authentication and accounting are insufficient then the risk of insufficient investigation of information compromise is increased*
    b. Mitigation: *Implementation of appropriate identity credential and access management (ICAM), IP address management (IPAM), account activity tracking and log review, hardware and software inventories, and incident response best practices*
7. Access Control
    a. Risk: *If appropriate or authorized access to information controls are insufficient then the risk of inappropriate or unauthorized access to information assets is increased*
    b. Mitigation: *Implementation of appropriate identity credential and access management (ICAM)*
8. Confidentiality, Integrity, & Availability
    a. Risk: *If confidentiality, integrity, and availability cybersecurity protection mechanisms are insufficient then the risk of a data breach and compromise of information assets is increased*
    b. Mitigation: *Cybersecurity implemented as a concept-to-disposition design requirement.*
9. Incident Response & Investigation
    a. Risk: *If Chain of Custody and processing of evidentiary information lacks rigor and fidelity then the risk of failed prosecution of criminal activity is increased*
    b. Mitigation: *Forensics expertise, Public Key Infrastructure (PKI) for non-repudiation, and investigative collaboration with law enforcement (arranged ahead of time of crisis)*

Key Points:

1. Data governance is significantly impacted by the complexity, risk, and scale of IPv6
2. Data governance cyber training applies to professionals, communities, and families
3. Continuity of information services is dependent of both IPv4 and IPv6
4. ICT modernization offers the opportunity to leap ahead of old technologies and close the digital divides (technical, infrastructure, knowledge, skills, and abilities (KSA), and cybersecurity)
5. ICT modernization offers the opportunity to bake-in cybersecurity as a design requirement
6. Technical complexity, risks, and operational costs can be reduced by migrating to simpler operations (in the past keeping IPv4 predominant, in the future driving IPv6 predominance)

IP Modernization Impact to Mobile Operations



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, 11th August 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.

Show 10 entries Search:

Rank	Participating Network	ASN(s)	IPv6 deployment
1	Comcast	7015, 7016, 7725, 7922, 11025, 13367, 13385, 20214, 21508, 22258, 22909, 33287, 33489, 33490, 33491, 33650, 33651, 33652, 33653, 33654, 33655, 33656, 33657, 33659, 33660, 33661, 33662, 33664, 33665, 33666, 33667, 33668, 36732, 36733	48.30%
2	ATT	6389, 7018, 7132	60.30%
3	KDDI	2516	26.06%
4	Verizon Wireless	6167, 22394	75.03%
5	Time Warner Cable	7843, 10796, 11351, 11426, 11427, 12271, 20001	30.00%
6	SoftBank	17676	14.52%
7	T-Mobile USA	21928	67.33%
8	Deutsche Telekom AG	3320	30.94%
9	British Sky Broadcasting	5607	71.69%
10	SKTelecom	9644	31.41%

Showing 1 to 10 of 268 entries

Percentage of Alexa Top 1000 websites currently reachable over IPv6

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

Apple Supporting IPv6-only Networks

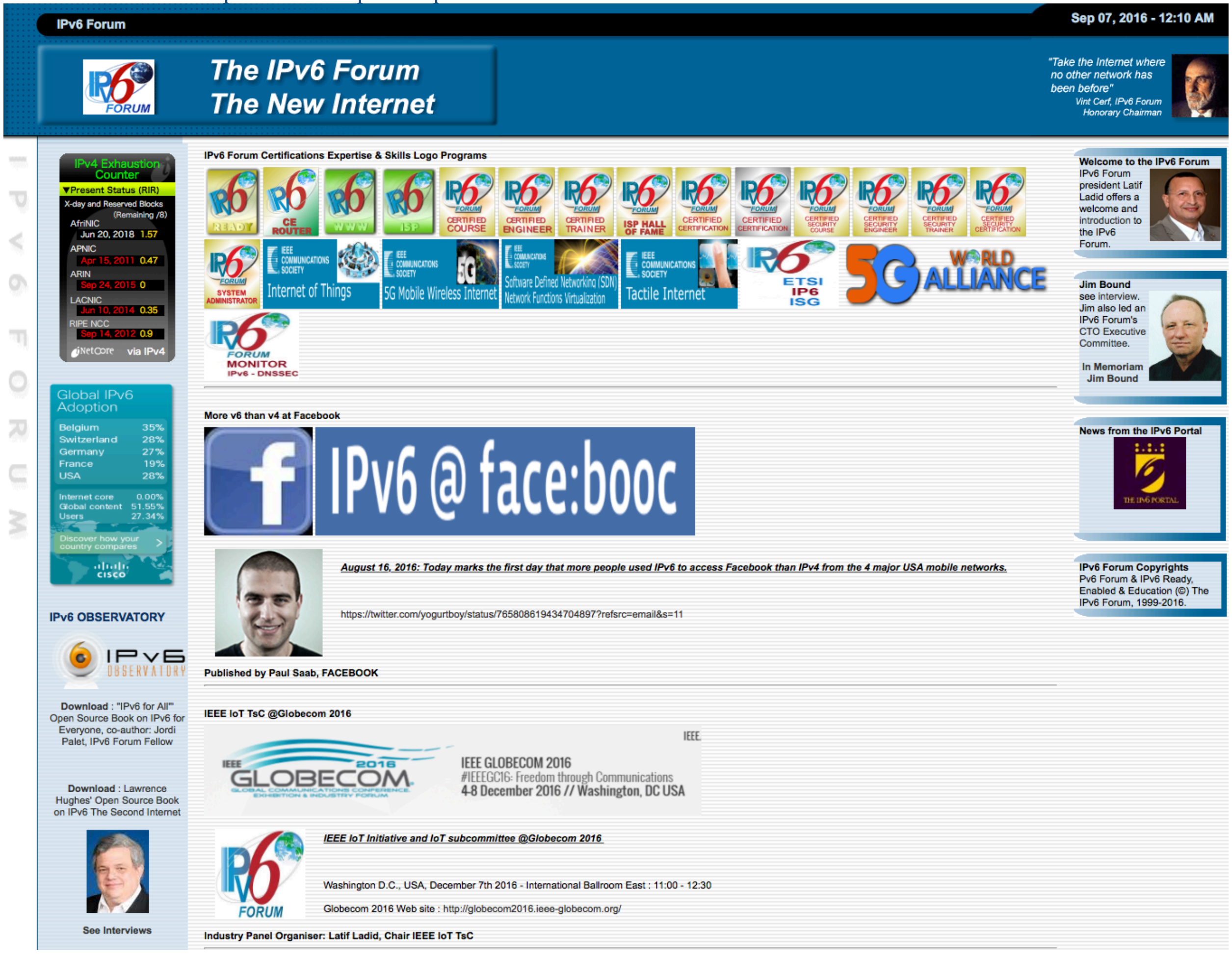
Starting June 1, 2016 all apps submitted to the App Store must support IPv6-only networking.
Source: https://developer.apple.com/news/?id=05042016a

Key Points:

1. The mobile carrier space is already IPv6 predominant
2. Consider mobile networks such as automobile fleets, unmanned aerial systems (UAS), and autonomous vehicles
3. Consider wireless (radio frequency) connectivity for IoT, mobile communications, emergency communications

Data Governance: ICT Modernization Impacts to Business Operations

IP Modernization Impact to Enterprise Operations



IPv6 Forum

Sep 07, 2016 - 12:10 AM

The IPv6 Forum
The New Internet

"Take the Internet where no other network has been before"
Vint Cerf, IPv6 Forum Honorary Chairman

IPv4 Exhaustion Counter

▼Present Status (RIR)

X-day and Reserved Blocks (Remaining /8)

AfriNIC	Jun 20, 2018	1.57
APNIC	Apr 15, 2011	0.47
ARIN	Sep 24, 2015	0
LACNIC	Jun 10, 2014	0.35
RIPE NCC	Sep 14, 2012	0.9

NetCore via IPv4

Global IPv6 Adoption

Belgium	35%
Switzerland	28%
Germany	27%
France	19%
USA	28%

Internet core	0.00%
Global content	51.55%
Users	27.34%

Discover how your country compares

IPv6 OBSERVATORY

Download : "IPv6 for All" Open Source Book on IPv6 for Everyone, co-author: Jordi Palet, IPv6 Forum Fellow

Download : Lawrence Hughes' Open Source Book on IPv6 The Second Internet

See Interviews

IPv6 Forum Certifications Expertise & Skills Logo Programs

More v6 than v4 at Facebook

August 16, 2016: Today marks the first day that more people used IPv6 to access Facebook than IPv4 from the 4 major USA mobile networks.

https://twitter.com/yogurtboy/status/765808619434704897?refsrc=email&s=11

Published by Paul Saab, FACEBOOK

IEEE IoT TsC @Globecom 2016

IEEE GLOBECOM 2016
#IEEEGC16: Freedom through Communications
4-8 December 2016 // Washington, DC USA

IEEE IoT Initiative and IoT subcommittee @Globecom 2016

Washington D.C., USA, December 7th 2016 - International Ballroom East : 11:00 - 12:30

Globecom 2016 Web site : http://globecom2016.ieee-globecom.org/

Industry Panel Organiser: Latif Ladid, Chair IEEE IoT TsC

Welcome to the IPv6 Forum
IPv6 Forum president Latif Ladid offers a welcome and introduction to the IPv6 Forum.

Jim Bound
see interview. Jim also led an IPv6 Forum's CTO Executive Committee.

In Memoriam
Jim Bound

News from the IPv6 Portal

IPv6 Forum Copyrights
Pv6 Forum & IPv6 Ready, Enabled & Education (©) The IPv6 Forum, 1999-2016.

Source: http://www.ipv6forum.org

ARIN IPv4 free-pool reaches zero
Source: https://www.arin.net/vault/announcements/2015/20150924.html

Related National Levels of Effort:

1. Federal Communications Commission National Broadband Plan
   Source: https://www.fcc.gov/general/national-broadband-plan
2. FirstNet National Public Safety Broadband Network
   Source: http://www.firstnet.gov
3. Federal Aviation Administration: The FAA's New Drone Rules Are Effective Today (posted 8/29/2016)
   Source: http://www.faa.gov/news/updates/?newsId=86305

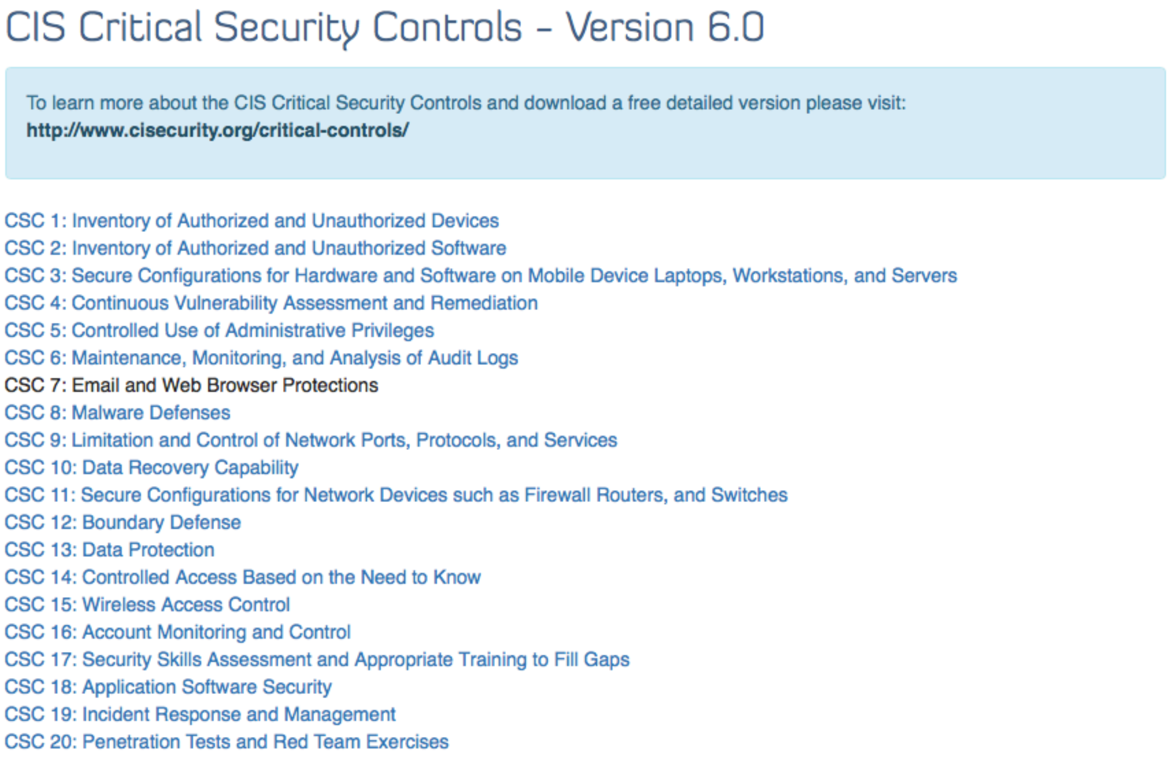
Key Points:

1. IPv6 is a worldwide adoption effort
2. Related efforts should consider the IP lifecycle transition to IPv6 for new and anticipated development

Best Practices

Guidelines for the Secure Deployment of IPv6, Special Publication 800-119
Source: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-119.pdf

SysAdmin, Audit, Network, Security (SANS) Institute



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

Source: https://www.sans.org/critical-security-controls

20 Critical Security Controls – Example Comments

The goal is equivalence in IPv4 and IPv6 protection posture. The following are suggested wording for IPv6.

CSC #1: Inventory of Authorized and Unauthorized Devices
System 1.1 (QW) Suggested Change:
Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public, private, mobile and adhoc (i.e. IPv6 stateless address auto-configuration (SLAAC)) network(s). Both active tools that scan through Internet protocol (IP) version 4 (IPv4) or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

CSC # 2: Inventory of Authorized and Unauthorized and Software
System 2.2 (QW) Suggested Change:
Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, laptops, and mobile devices of various kinds and uses including IPv4 and IPv6 approved and tested operating systems and stacks.

CSC # 3: Secure Configurations of Hardware and Software
System 3.4 (C/H) Suggested Change:
Do all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as IPv4 or IPv6 based telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS, or IPSEC.

Data Governance: ICT Modernization Impacts to Business Operations

ICT Modernization Best Practices

Drivers: IPv6 Enabled External and Internal ICT Services, Cybersecurity

Technical Phase I - Enterprise implementation based on NIST SP 800-119:

Technical Phases	Tasks
Initiation	#1 Develop Baseline IPv6 Knowledge
	#2 Hardware Inventory
	#3 Software Inventory
	#4 Service Inventory
	#5 Operational Support Tools Inventory
	#6 Cybersecurity Tools Inventory
Acquisition/Deployment	#7 Information Service and Application Upgrade Planning
	#8 IPv6 Numbering Plan
	#9 Conduct IPv6 Application and Function Test and Evaluation
	#10 Infrastructure and Service Operations Upgrade Plan
	#11 Internal Network Dual-Stack Upgrade Plan
	#12 Cost Analysis
Implementation	#13 Build an IPv6 Test Bed
	#14 Cybersecurity Architecture and Design
	#15 Update Firewalls for IPv6
	#16 Enable DMZ’s for IPv6
	#17 Enable External DNS for IPv6
	#18 Enable External WWW for IPv6
	#19 Enable External Email for IPv6
	#20 Enable Other Outbound Services and Applications for IPv6
	#21 Enable Internal Services and Applications for IPv6
Operations/Maintenance	#22 Upgrade IP Address Management (IPAM) for IPv6
	#23 Enable Active Directory or LDAP and ICAM Services
	#24 Develop Systems Management for IPv6
	#25 Network Monitoring for IPv6
Disposition	Legacy IP Migration Displacement and Retirement of Equipment

ICT Modernization and Mobile Operations

Drivers: IP/RF Mobile Computing, Mobile Networks, Life-Line Services, Cybersecurity

Technical Phase II – Mobile implementation estimation of ICT modernization and NIST SP 800-119 best practices:

Technical Phases	Tasks
Initiation	#1 Develop Mobile IPv6 Knowledge
	#2 Add Mobile to Hardware, Software, and Service Inventories
	#3 Mobile Support Tools Inventory (Interoperability, Geo-Location, NG-911)
	#4 Mobile Cybersecurity Tools Inventory
Acquisition/Deployment	#5 Mobile Services and Application Upgrade Planning
	#7 Mobile IPv6 Numbering Plan
	#8 Conduct Mobile IPv6 Application and Function Test and Evaluation
	#9 Mobile Infrastructure and Service Operations Upgrade Plan
	#10 Mobile Network Upgrade Plan
	#11 Mobile Device and Service Cost Analysis
Implementation	#12 Enable External DNS for Mobile IPv6
	#13 Upgrade IP Address Management (IPAM) for Mobile IPv6
	#14 Enable LDAP and ICAM Services for Mobile IPv6
Operations/Maintenance	#15 Develop Systems Management for Mobile IPv6
	#16 Network Monitoring for Mobile IPv6
Disposition	#17 Legacy Mobile IPv6 Migration Displacement and Retirement of Equipment

Risk Management

SNL Risk Management Framework Example

The context of mitigations for IPv6 deployment minimizes overall risk level as compared to unmitigated risk levels. Risk statements are framed in if/then statements for consistent representation and alignment. The general format is illustrated below:

FORMAT: Risk - Risk Category - Inherent Risk Level – Mitigation – Test/Verification - Mitigated Risk Level

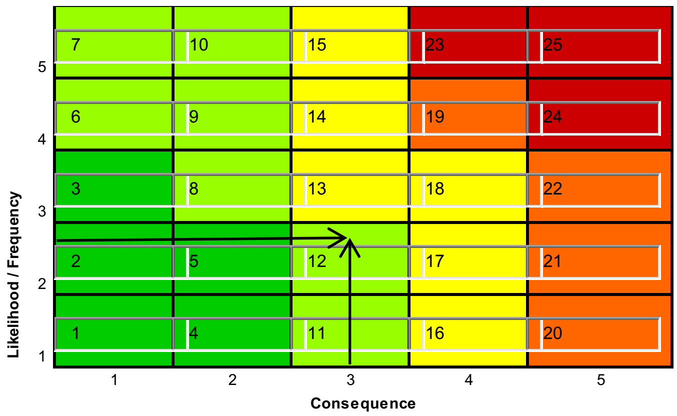
Inherent (unmitigated) and residual (mitigated) risk values are illustrated in heat maps. Risk scores are derived from Inherent and residual risk levels by indicating estimated likelihood and anticipated consequence.

Likelihood	Probability of Occurrence
1 - Rare	0 <= X < 20%
2 - Unlikely	21% < X < 40%
3 - Possible	41% < X < 60%
4 - Likely	61% < X < 80%
5 - Almost Certai	81% < X <= 100%

Levels of consequence describe risk as follows:

Score	Descriptor
5	Catastrophic/Critical
4	Major
3	Moderate
2	Minor
1	Insignificant

Inherent risk scores are represented as likelihood and consequence before measures are put in place to reduce risk to an acceptable level. Residual risk scores are represented as likelihood and consequence after measures are put in place to reduce risk to an acceptable level. Ex: If a risk is determined to have a Likelihood of 2 Unlikely and a Consequence of 3 Moderate the risk score is a 12.



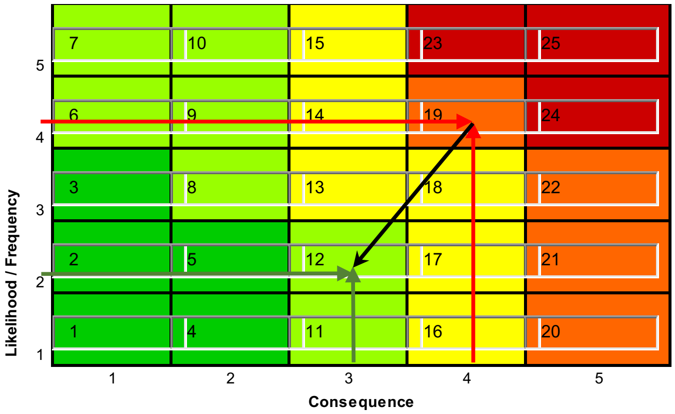
Risk Reference: http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
SP800-119 describes operational practices to prevent security exposure in enterprise networks resulting from unplanned use of IPv6. Widespread deployment and growth of networking technologies and mobile communications have surpassed IPv4's ability to provide adequate globally unique address space.

Risk Reference: [8] https://tools.ietf.org/html/rfc7123
IETF RFC 7123, Security Implications of IPv6 on IPv4 Networks, February 2014, describes operational practices to prevent security exposure in enterprise networks resulting from unplanned use of IPv6.

Technical Risk Example

Risk: If dynamic tunneling mechanisms (Teredo, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 6to4, Tunnel Setup Protocol (TSP), Anything-in-Anything (AYIYA)) are leveraged to evade security controls, then covert or back channel may be established undetected.
Risk Category: Technical
Inherent Risk Level: Likely (4)/Major (4): 19
Mitigation: Apply desktop configuration control, service configuration control, and network traffic controls:
Block IPv4 Protocol 41 (ISATAP, 6to4, TSP, 6rd)
Block IPv4 destination prefix 192.88.99.0/24 (6to4)
Block IPv6 source prefix 2002::/16 (6to4)
Block IPv4 destination prefix 239.0.0.0/8 (6over4)
Disable DNS (A record) resolution to isatap.<localdomain> (ISATAP)
Block udp port 3544 (Teredo)
Disable DNS domain name (A record) resolution to teredo.ipv6.microsoft.com (Teredo)
Block tcp, udp 3653 (TSP)
Block tcp, udp 5072 (AYIYA)
Tests/Verification: Verify and validate access control list (ACL), network firewall, personal firewall, and application firewall configuration compliance.
Residual Risk Level: Likely (2)/Moderate (3): 12

Inherent and Residual Heat Map



Inherent Risk ↔ Residual Risk ↔

This approach addresses three risk categories of risk:
1. Technical – Engineered Controls
2. Operational – Process and Procedural Controls
3. Administrative – Legal, Policy and Compliance Controls

Risk Management Frameworks

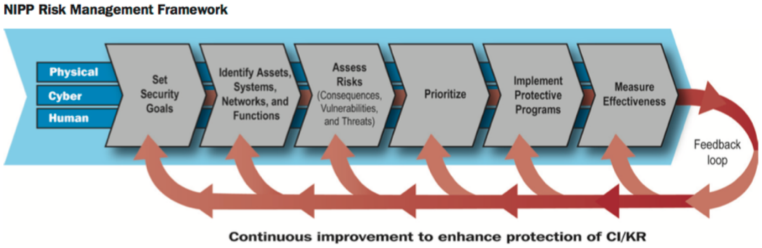
Sandia National Laboratories has also developed a risk informed management model that combines quantitative risk (value vs. cost) and qualitative risk (difficulty of attack) to facilitate science and engineering based cyber capabilities.

[8] Internet Engineering Task Force (IETF) Request for Comments: 7123, Category: Informational, ISSN: 2070-1721, February 2014
F. Gont, SI6 Networks/UTN-FRH, W. Liu, Huawei Technologies

Data Governance: ICT Modernization Impacts to Business Operations

Risk frameworks vary with the context of what is at risk. Additionally, risk management may require culture change and executive championship to successfully achieve desired outcomes. Important examples include:

1. National Infrastructure Protection Plan (NIPP) Risk Management Framework, 2013


NIPP Risk Management Framework
Physical
Cyber
Human
Set Security Goals
Identify Assets, Systems, Networks, and Functions
Assess Risks (Consequences, Vulnerabilities, and Threats)
Prioritize
Implement Protective Programs
Measure Effectiveness
Feedback loop
Continuous improvement to enhance protection of CI/KR

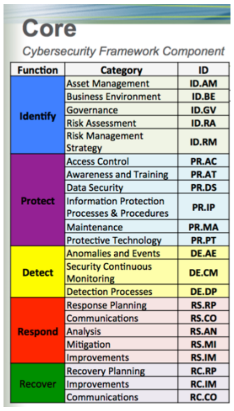
Source: https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf

Note: NIPP Security and Resilience Challenge, 2016

2. The National Security Communications Plan, NSCP 2014
   Source: https://www.dhs.gov/national-emergency-communications-plan
3. The 2014 NIST Risk Management Framework provides guidance for federal, state, tribal, territorial, and local governments as well as the private sector. The following is a truncated summarization:

   Step 1: Categorize
   Categorize the information system and the information processed, stored, and transmitted by that system.
   Step 2: Select
   Select baseline security controls for the information system based on the security categorization.
   Step 3: Implement
   Implement security controls and document how the controls are deployed within the information system.
   Step 4: Assess
   Assess that controls are implemented correctly, operating as intended, and producing the desired outcome.
   Step 5: Authorize
   Authorize information system operation based upon the risk to organizational operations and assets, individuals, other organizations and the Nation.
   Step 6: Monitor
   Monitor and assess selected security controls in the information system on an ongoing basis.

   Source: http://csrc.nist.gov/groups/SMA/fisma/framework.html
4. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, January, 2016



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

Source: http://csrc.nist.gov/groups/SMA/forum/documents/january2016_presentations/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf

Key Points:

1. Technical risks can be mitigated with a knowledgeable workforce, best practices, and engineered controls.
2. Organizational risks can be mitigated with workforce KSA's, and process controls.
3. Administrative risks can be mitigated with administrative controls, enforcement of policies, and compliance with designated approving authorities.
4. Chose what's the right risk management approach for your organization – there are several great models.

Data Governance: ICT Modernization Impacts to Business Operations

IPv6 Deployment Case Scenario

Justification:
Why IP modernization? IPv6 is necessary for growth and continuity of information service delivery.
What's the impact? IPv6 is a fundamental enabler for all things Internet to come.

Heilmeier's Catechism:
How is it done today what are the limits of current practices?
The IPv4 available free pool address space is exhausted.

What's new and why will it be successful?
IPv6 adoption is world-wide and inevitable for continuity of the Internet information services.

Who care's?
Internet service providers, telecom carriers, information service providers, cybersecurity practitioners.

What difference will it make?
Continued ICT and internet innovation – emergency communications, smart grid…

What are the risks and payoffs?
The risk of delay is gradual loss of connectivity with IPv6 enabled information assets on the Internet; the risk of adoption is increased complexity, risks, and costs. Complexity, risks, and costs can be minimized with a cyber-centric approach and single-stack IPv6 design goals. The payoffs are business continuity through modernized ICT and internet services; ecommerce development opportunities.

How much will it cost?
Initial costs are associated with training to develop a knowledgeable workforce. Typical training cost for a class of 30 technical students is estimated at $30,000. If computing and network infrastructure is modernized circa 2010 than your ICT infrastructure is predominately IPv6 capable, if not than technology acquisition investments will need to be made. Eventually IPv6 operations and security become part of day-today information service operations.

How long will it take?
IPv6 adoption is for the foreseeable future.

What are midterm and final exams to check for success?
1) IPv6 security, and external service capability, 2) dual-stack internal functional capability, and 3) eventual single-stack IPv6 enabled ICT infrastructure.

Design Requirements

1. IPv6 is an enabling technology for growth and must be designed into information and communication technology solutions including mobility, cloud, software defined networks and the Internet of Things (IoT).
2. Security is a design requirement from concept to disposition.

Key Design Principals

1. Extensibility: Accommodate anticipated and unanticipated future IPv6 utilization.
2. Resiliency: Critical services, systems and security designed for redundancy and recovery where appropriate.
3. Business continuity: Utilize IPv6 to sustain continuity of information services.
4. Security: Cybersecurity will be "baked-in" by design for a sustainable and resilient protection posture.

Data Governance: ICT Modernization Impacts to Business Operations

Internet Threat Review

This is a representative list rather than an exhaustive list of Internet threats. Information sources include IPv6 Security: ISBN-13 978-1-58705594

IPv6 Internet Threats	Mitigations
Packet Flooding	Network Perimeter Filtering, Rate Limiting
Internet Worms	Network Perimeter Filtering, Intrusion Detection System (IDS), Virus Protection
Distributed Denial of Service (DDOS)	Network Perimeter Filtering, Intrusion Detection System (IDS), Rate Limiting
Man in the Middle	Encryption, Generic Routing Encapsulation (GRE), IPSec Virtual Private Networks (VPN)
Botnets	Network Perimeter Filtering, Intrusion Detection System (IDS), Data Loss Prevention (DLP)
Bogon Addresses	Network Perimeter Filtering
BGP TTL, Long As paths, Private AS paths	Network Perimeter Filtering, BGP Authentication, Hop Limit set to 255 - Generalized TTL-based Security Mechanism (GTSM)
IGP Prefix Delegation Threats	Network Perimeter Filtering, Intrusion Detection System (IDS)
SLAAC Predictability	Dynamic Host Configuration Protocol (DHCPv6), Cryptographically Generated Addresses (CGA), Randomly Generated Addresses, Manually Configured Addresses
Multi-homing Issues	Provider Independent (PI) IPv6 address Allocation as opposed to Provider Aggregatable (PA) IPv6 address Allocation, Site Multihoming by IPv6 Intermediation (SHIM6)

Cybersecurity Architecture Example: 2001:DB8::/64

External/Internet
(*ISP*)
|
EN Data Regime
External Demarcation Zone (DMZ)
External Facing Services
Partner Connectivity
Internal DMZ
|
---**Separate Internal Data Regimes**---

|	|	|	|	|	|	|
Remediation & Test	Public	Anchor Institutions	Government	IT/Telecom	Datacenter	Business Operations
DMZ	DMZ	DMZ	DMZ	DMZ	DMZ	DMZ
Cyber Systems	Cyber Systems	Cyber Systems	Cyber Systems	Cyber Systems	Cyber Systems	Cyber Systems
Best Practices	**Best Practices**	**Best Practices**	**Best Practices**	**Best Practices**	**Best Practices**	**Best Practices**
Services	Services	Services	Services	Services	Services	Services

External Attack Surface Case Scenario: 2001:DB8:[0]000-FFF]:[0000-FFFF]::/64

|**External Demarcation Zone (DMZ): Technical Attack Surface**

|Internet

|Inter-site

|

|**Cyber Systems: Insider Attack Surface**

|Intrusion Detection systems

|Firewalls/Access Control Lists

|Intrusion Prevention Systems

|Application Layer Gateways/Proxies

|Data Loss Prevention

|Cyber Analysis

|Incident Response

|Logging

|

|**Internal Demarcation Zone (DMZ): Trust Attack Surface**

|Landing Zone for Internal DMZ’s

|

|**Partnership Networks: Attack Surface of Others**

|Inter-jurisdictional

|

|**Test & Evaluation: Adjacent Attack Surface**

|New Technologies

|Compliance

|

|**Remediation & Isolation: Malware Attack Surface**

|Quarantine

|Malware Analysis

|Scanning & Patching

|

|**External Facing Services: Application Attack Surface**

|Email

|Web

|DNS

Data Governance: ICT Modernization Impacts to Business Operations

Data Categorization & Continuity Case Scenario: 2001:DB8:[2]000-FFF]:[0000-FFFF]::/64

|**Internal Demarcation Zone (DMZ): Insider Information**
|DMZ (Remote Access)
|**Cyber Systems: Proprietary & Privileged Information**
|Intrusion Detection systems
|Firewalls/Access Control Lists
|Intrusion Prevention Systems
|Application Layer Gateways/Proxies
|Data Loss Prevention
|Incident Response
|Logging & Analysis
|**Government Operations: Statutory & Public Information**
|Executive
|Judicial\Law Enforcement
|Appropriations
|**Continuity of Government (CoG)**
|**Anchor Institutions: Personally Identifiable Information**
|**Emergency Management**
|Health
|Education
|Community Services
|**Business Continuity Planning (BCP)**
|**Business Operations: Commercial Information**
|Ecommerce
|Energy
|Finance
|**Continuity of Operations Planning (COOP)**
|**IT & Telecom Common Core Services: Privileged Information**
|Domain Name System (DNS)
|Network Time Protocol (NTP)
|IP Address Management (IPAM)
|Identity and Credential Management (ICAM)
|Dynamic Host Configuration Protocol, version 6 (DHCPv6)
|Directory Services/Lightweight Directory Access Protocol (LDAP)
|VoIP
|Video
|Geo-Location
|Cloud
|Mobility (5G and Internet of Things are coming fast!)
|Hardware Inventory
|Software Inventory
|**IT Disaster Recovery (ITDR)**
|**Operational Support Systems: Sensitive Information**
|Monitoring/Network management System
|System operations Center
|Network Operations Center
|Help Desk
|Critical Services
|**Corporate App Services: Technical Information**
|Email
|Web

Data Governance: ICT Modernization Impacts to Business Operations

Sandia National Laboratories

1. Must meet national security objectives to conduct work with non-federal entities
2. Serves as an objective advisory for critical infrastructure concerns
3. Does not compete with industry

Science and Engineering Based Cyber Capabilities

	Science & Engineering Based Cyber Interdisciplinary Expertise
Assessment	**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.
Analysis	**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.
Training	**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.
Design	**Design Technical Assistance** – Energy efficiency, facilities, and information service technical assistance with design/build guidance to enhance development of emergent next generation services tailored to customer needs.
Engineering	**Cyber Safeguard Engineering and Tech Transfer** - 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, simulation, and emulytics 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

References

American Registry for Internet Numbers (ARIN)
https://www.arin.net

IPv6 Forum
http://www.ipv6forum.org

IPv6 Measurements
http://www.worldipv6launch.org/measurements/

Internet Society
https://www.internetsociety.org/blog/tech-matters/2015/03/rough-guide-ietf-92-all-about-ipv6

National Institute of Standards and Technology (NIST)
http://www.nist.gov/itl/antd/usgv6.cfm
Guidelines for the Secure Deployment of IPv6, Special Publication 800-119
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-119.pdf
IPv6 Deployment Tracker
https://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov
Guide for Applying the Risk Management Framework to Federal Information Systems, Special Publication 800-37
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Internet Engineering Task Force (IETF)
Network Working Group Request for Comments (RFC) 2460, Internet Protocol, Version 6 (IPv6) Specification
https://tools.ietf.org/html/rfc2460
RFC 4291, IP Version 6 Addressing Architecture
https://tools.ietf.org/html/rfc4291
RFC: 1881 "IPv6 Address Allocation Management", December 1995
https://tools.ietf.org/html/rfc1881
RFC: 2401 "Security Architecture for the Internet Protocol", November 1998.
http://www.rfc-editor.org/rfc/rfc2401.txt
Requirements for IPv6 Enterprise Firewalls
https://datatracker.ietf.org/doc/draft-gont-opsec-ipv6-firewall-reqs/

SysAdmin, Audit, Network, Security (SANS) Institute
https://www.sans.org
CIS Critical Security Controls for Effective Cyber Defense
https://www.sans.org/critical-security-controls

Internet Information System Security Professional Consortium ((ISC)^2)
https://www.isc2.org
Center for Cyber Safety and Education
https://www.isc2cares.org/Default.aspx

Federal Trade Commission
Privacy, Identity, & Online Security
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
https://www.consumer.ftc.gov/blog/what-your-phone-telling-your-rental-car

Cisco Press
Deploying IPv6 Networks: ISBN-13-1-58705-210-5
http://www.ciscopress.com/store/deploying-ipv6-networks-9781587052101
IPv6 Security: ISBN-13 978-1-58705594
http://www.hoggnet.com/ , http://www.ciscopress.com/store/ipv6-security-9781587055942