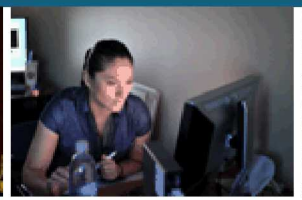
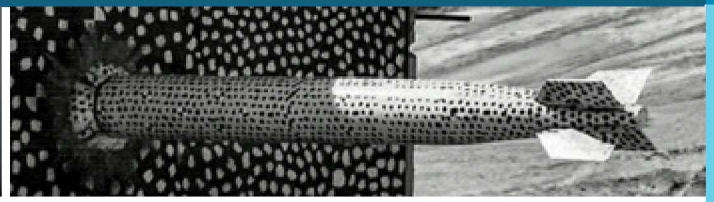
SAND2018-10039C

Broadband, Information Technology, and Operational Technology Multidomain Security





Sand Report #

PRESENTED BY

Curtis Keliiaa at the (ISC)^2 2018 Security Congress

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Session Overview

Broadband (BB), Information Technology (IT), and Operational Technology (OT) are are inextricably linked in worldwide connectivity expansion

The modernization and integration of BB-IT-OT imposes a vast scale of connectivity with new technologies, functions, and security challenges

The resultant impact crosses all domains with information and communications technology dependencies

A standards-based risk management approach and path-forward for cybersecurity, physical-security, and resilience is presented

Discussion will include recommendations for securing a changing cyber ecosystem

The goal is to address cutting-edge opportunities and challenges with multi-domain protection, security, and resilience

Learning Objectives

To understand:

broadband, IT, and OT multi-domain security challenges;

how to apply integrated cybersecurity, physical security, and resilience design principles;

the rapidly changing cyber ecosystem;

deliver leap ahead technological advantage for multi-domain standards-based risk management;

application of confidentiality, integrity, and availability security design principles in OT and IT systems; and

enhanced information protection at-rest, in-transit, and in-process

Introduction to Computing at Sandia National Laboratories

High Performance Computing

Funding profiles for Scientific Computing at Sandia:

1. NNSA Advanced Simulation and Computing
2. Institutional Computing program
3. DOE Office of Science, Advanced Scientific Computing Research

ASC Tri-Lab Networks/Systems at SNL, LANL and LLNL:

- Continuous Access to Large Compute Systems
- ~60PF, ~10B Processor Hours/Year

Operations:

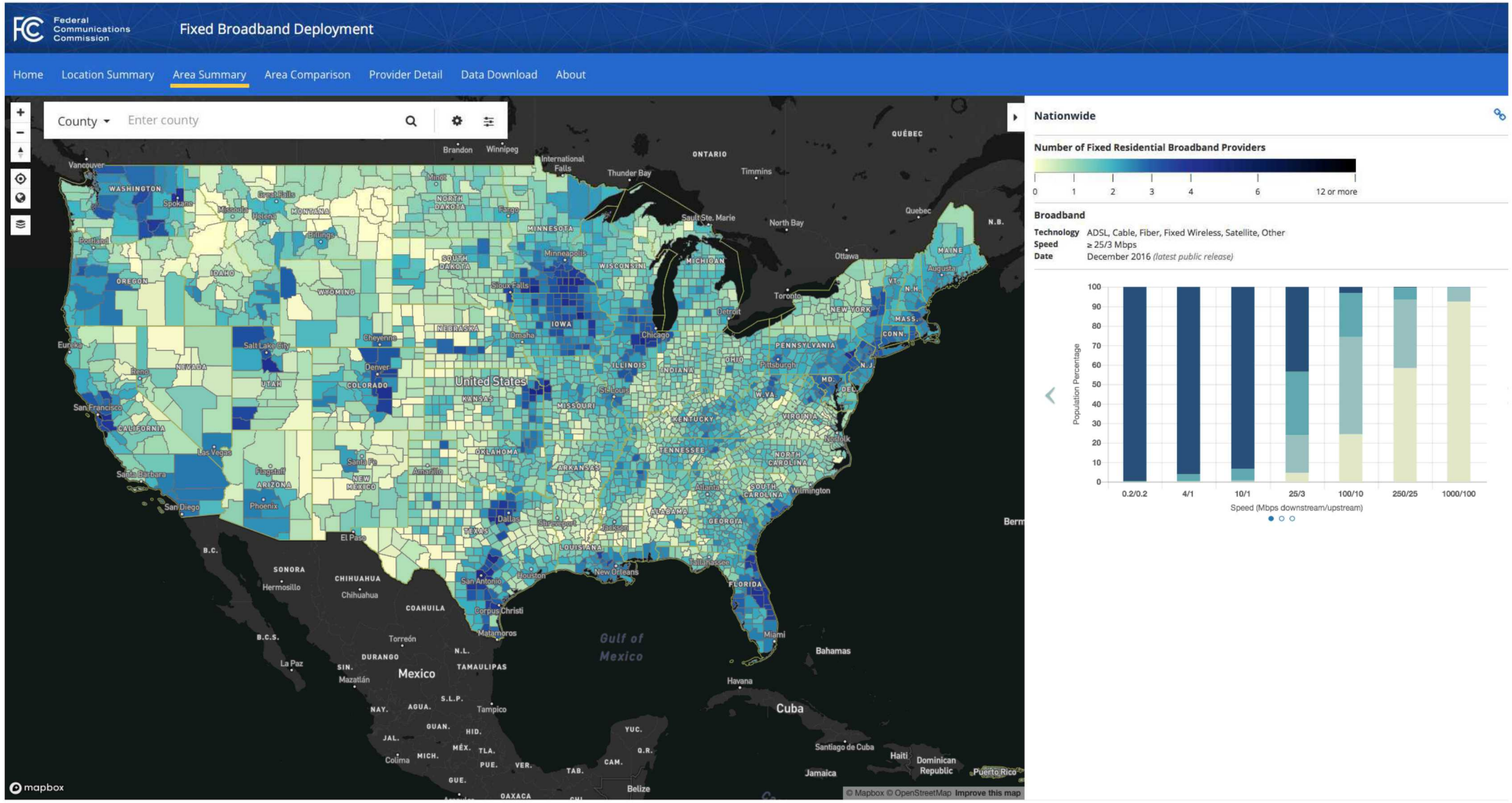
- Scientific Computing Platforms – 14 clusters in 4 environments
- System Acquisition, Maintenance & Operations
- High Speed Parallel File Systems
- High Performance Parallel Networks
- Multi-Petabyte Data Archive Systems
- Facilities Improvements
- User Support Personnel
- Analysts & Code Development

Center for Computing Research

Computing research focused on cross-cutting challenges and enabling capabilities:

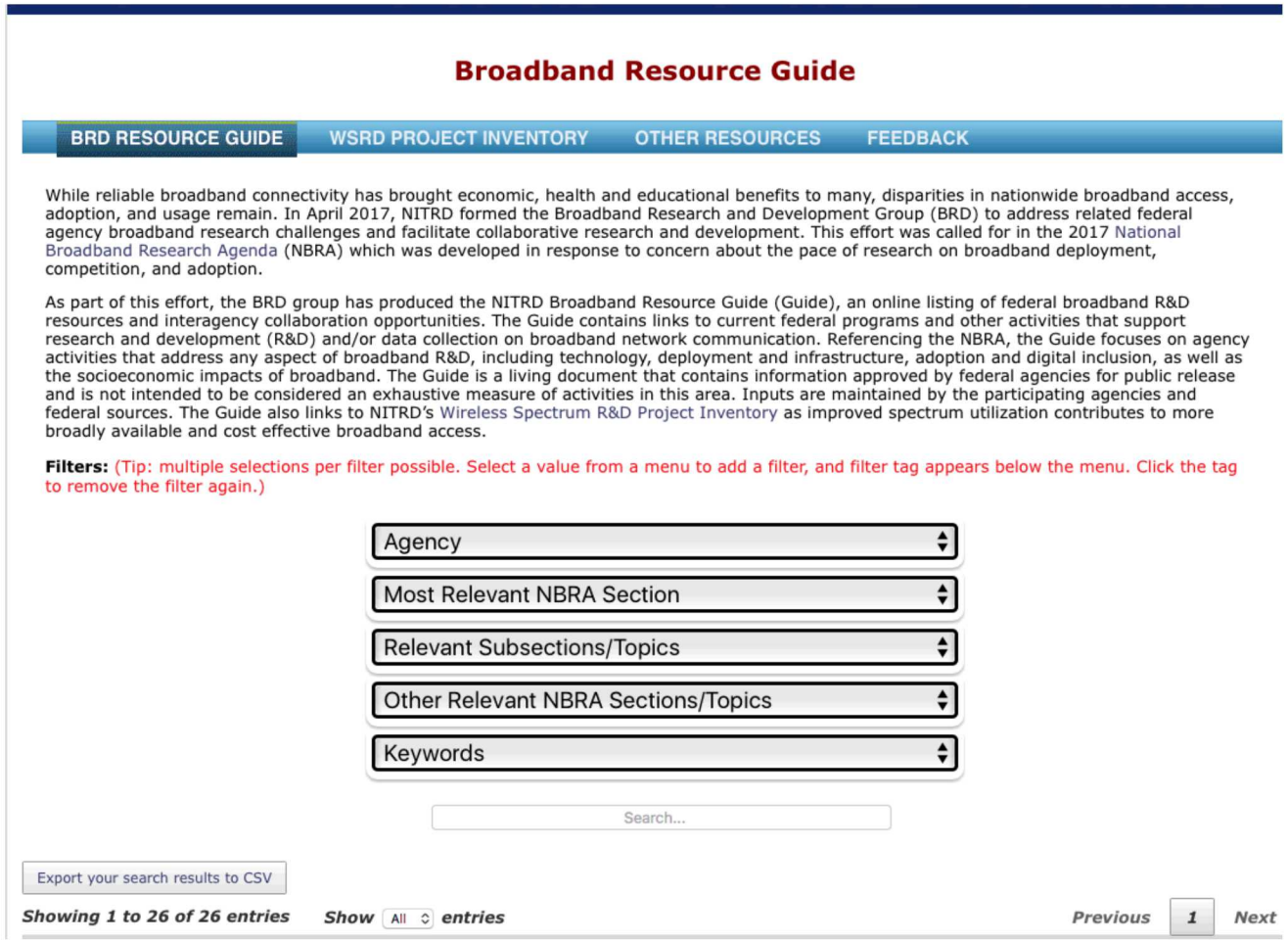
- Streaming algorithms to process large data streams
- Algorithms to find patterns in large graphs
- Machine learning techniques to detect adversarial behavior (e.g. phishing emails)
- Quantum Information Systems
- Cognitive Science
- Neural Networks
- Cyber Emulytics
- Exascale Computing
- Remote sensing challenges
- Cybersecurity Engineering Research Institute Collaboration with Industry and Academia

Broadband

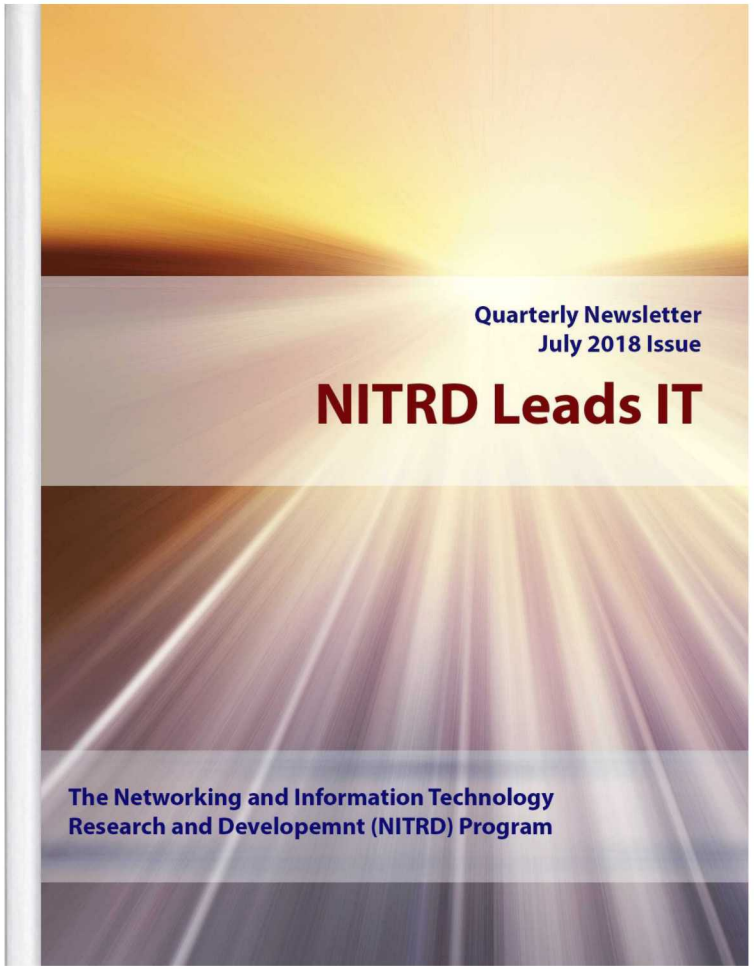


Source: Federal Communications Commission National Broadband Map, accessed 8/21/2018; https://broadbandmap.fcc.gov/#/area-summary

Networking and IT Research and Development Program: Broadband Resource Guide

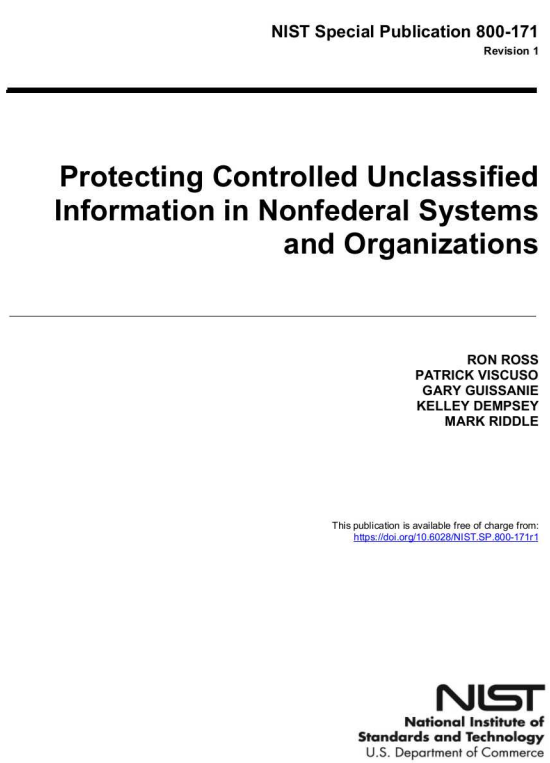


Source: https://www.nitrd.gov/apps/broadband/



Source: https://www.nitrd.gov/pubs/newsletter/NITRD-Newsletter-07162018.pdf

Information Technology Security



NIST Special Publication 800-171
Revision 1

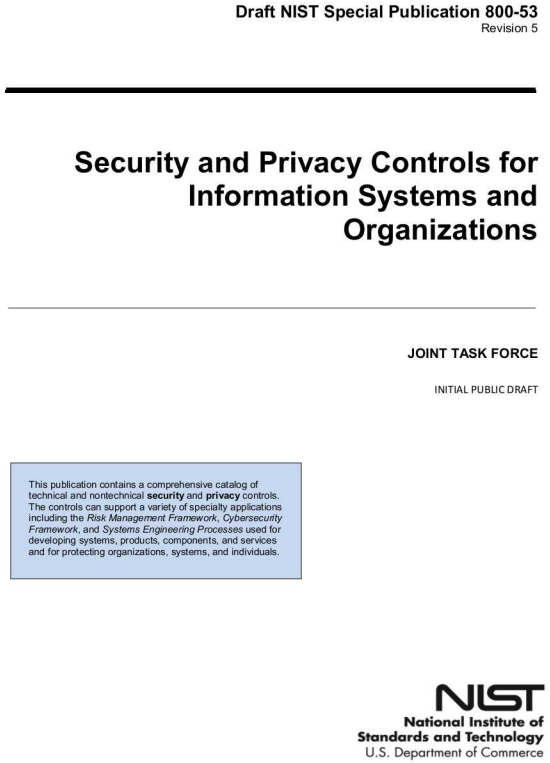
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Source: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final



Draft NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

INITIAL PUBLIC DRAFT

This publication contains a comprehensive catalog of technical and nontechnical **security** and **privacy** controls. The controls can support a variety of specialty applications including the *Risk Management Framework*, *Cybersecurity Framework*, and *Systems Engineering Processes* used for developing systems, products, components, and services and for protecting organizations, systems, and individuals.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

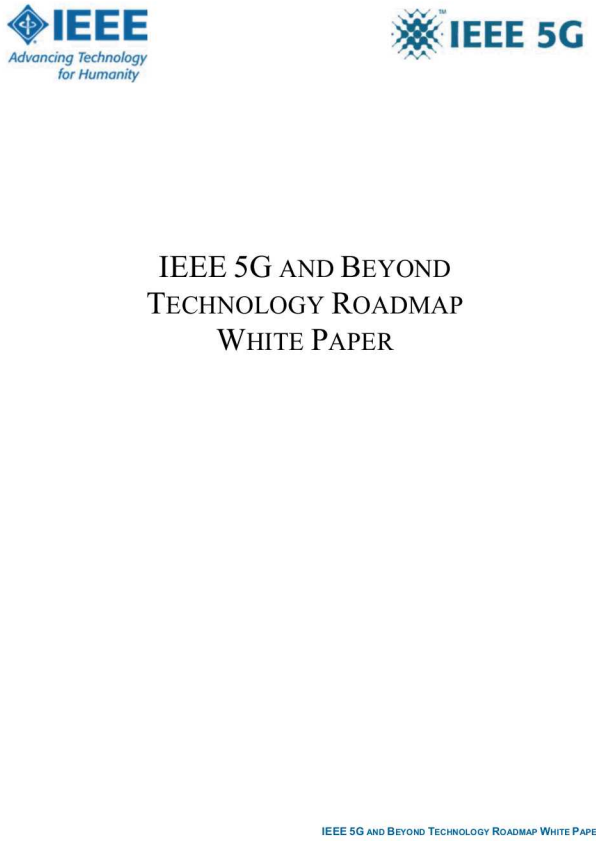
Source: https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

NIST SP 800-53, Rev 5

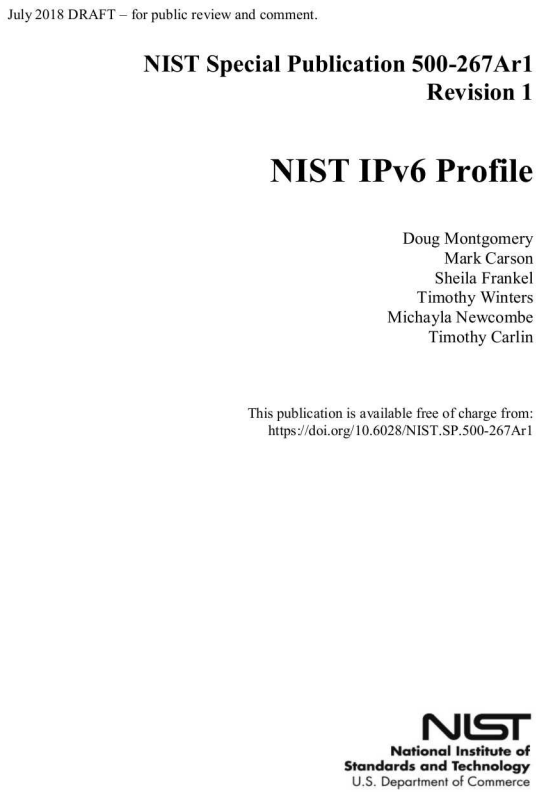
Abstract

This publication provides a catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, Executive Orders, directives, regulations, policies, standards, and guidelines. *The publication describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions and business functions, technologies, environments of operation, and sector-specific applications.* Finally, the consolidated catalog of controls addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms) and an assurance perspective (i.e., the measure of confidence in the security or privacy capability). Addressing both functionality and assurance ensures that information technology products and the information systems that rely on those products are sufficiently trustworthy.

Communications Security



Source: https://5g.ieee.org/images/files/pdf/ieee-5g-roadmap-white-paper.pdf



Source: https://www.nist.gov/sites/default/files/documents/2018/07/12/draft-nist-sp-500-267ar1.pdf

Internet Protocol, version 6

ARIN IPv4 Free Pool Reaches Zero

Posted: Thursday, 24 September 2015

On 24 September 2015, ARIN issued the final IPv4 addresses in its free pool. ARIN will continue to process and approve requests for IPv4 address blocks. Those approved requests may be fulfilled via the Wait List for Unmet IPv4 Requests, or through the IPv4 Transfer Market.

Exhaustion of the ARIN Free Pool does trigger changes in ARIN's Specified Transfer policy (NRPM 8.3) and Inter-RIR Transfer policy (NRPM 8.4). In both cases, these changes impact organizations that have been the source entity in a specified transfer within the last twelve months:

> "The source entity (-ies within the ARIN Region (8.4)) will be ineligible to receive any further IPv4 address allocations or assignments from ARIN for a period of 12 months after a transfer approval, or until the exhaustion of ARIN's IPv4 space, whichever occurs first."

Effective today, because exhaustion of the ARIN IPv4 free pool has occurred for the first time, there is no longer a restriction on how often organizations may request transfers to specified recipients.

In the future, any IPv4 address space that ARIN receives from IANA, or recovers from revocations or returns from organizations, will be used to satisfy approved requests on the Waiting List for Unmet Requests. If we are able to fully satisfy all of the requests on the waiting list, any remaining IPv4 addresses would be placed into the ARIN free pool of IPv4 addresses to satisfy future requests.

ARIN encourages customers with questions about IPv4 availability to contact hostmaster@arin.net or the Registration Services Help Desk at +1.703.227.0660.

Regards,

John Curran
President and CEO
American Registry for Internet Numbers (ARIN)

Source:
https://www.arin.net/vault/announcements/2015/20150924.html

Source, Accessed 8/27/2018: http://www.ipv6forum.com

High level guidance documents often do NOT convey the duplicity of two IP versions, referring to "IP" in a singular context,

when in fact dual-stack is embedded in all fixed and mobile platforms

The two versions are distinctly different in function, and vastly different in scale!

www.nist.gov/news-events/news/2018/07/nist-releases-draft-revisions-usgv6-program-public-comment

NIST Releases DRAFT Revisions to USGv6 Program for Public Comment

Comments due by September 14, 2018.

July 12, 2018

DRAFT USGv6 Revision 1 Specifications Available for Public Comment

The first version of the of the USGv6 standards profile was published in 2008 and the USGv6 test program became operational in 2009. In the years since the USGv6 Program (as the effort is commonly known) has been referenced in Federal Acquisition Regulations, used as the basis for USG Agency strategic plans and acquisition policies and has resulted in the detailed documentation and test of IPv6 capabilities in a large number of commercial products.

This first major revision of the USGv6 program updates the standards profiles and testing program to achieve several goals:

1. To update the set of Internet Engineering Task Force (IETF) specifications that form the basis for the USGv6 profile to their latest published version.
2. To add new specifications for important IPv6 capabilities that have been developed since the publication of the first profile.
   - Highlights of these additions include technologies to support emerging use cases such as the Internet of Things, new forms of IPv6 transition technologies necessary to support "IPv6 Only" environments, and better support for specification of IPv6 enabled applications.
3. To remove specifications for IPv6 capabilities included in the first version of the profile but that has since failed to achieve significant support in commercial products and network deployments.
4. To update and consolidate the description of the USGv6 Test Program to reflect the lessons learned in the operation of that program to date.
   - Highlights of these changes include a more concise and consistent notation for

Source: https://www.nist.gov/news-events/news/2018/07/nist-releases-draft-revisions-usgv6-program-public-comment

Internet Protocol Transition: Old + New to New Only

Internet Protocol, version 6 enables growth and innovation

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[3], ICMP[4], other protocols	NDP[5], ICMPv6
Minimum MTU[6]	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[7] Identifiers	One subnet/VLAN ID per interface	Multiple subnet/VLAN ID's per interface
Address configuration	Manually, DHCP[8]	SLAAC, DHCP

Legacy IPv4

Table 1 Primary IPv4 and IPv6 Differences

Detailed IPv6 address architecture information can be found in rfc 4291, IP Version 6 Addressing Architecture: https://tools.ietf.org/rfc/rfc4291.txt

Dual Stack Purgatory

IPv6 (Only) Reduces Threat Surface IT and OT

The mobile and fixed wireless industry has enjoyed tremendous growth over the past decades. Indeed, mobile has evolved from a niche technology, embodied by an analog 1G voice system, to a full-fledged internet on the move and end-to-end (E2E) digital 4G system. *Now 5G communities—with many R&D, standardization, academia, fora, etc., around the globe—are aiming to fulfill demands (and hype) with a broad set of new technologies and capabilities being developed.*

So, what is beyond 5G?

One area will be software defined network/network function virtualization (SDN/NFV) to expand to E2E frameworks with distributed system software to enable all systems from management and control to user equipment (UE). Software-based design (i.e., softwarization) is a transformation that is not expected to be complete in the 5G timeframe.

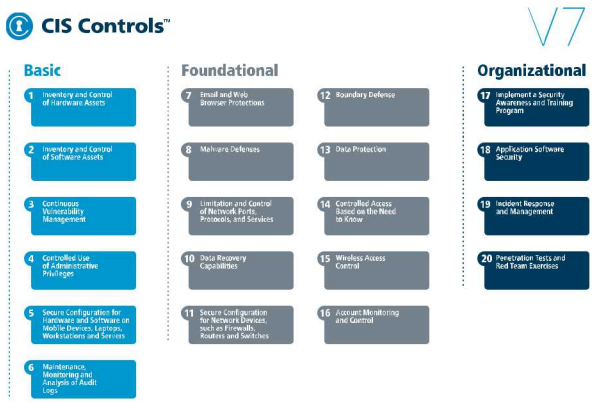
Protection At Rest, In Transit, and In Process

CIS Center for Internet Security

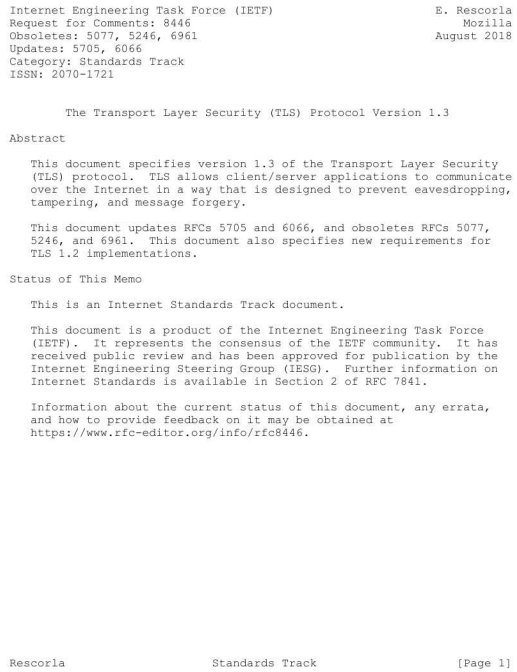
CIS Controls

CIS Controls™

Version 7



Source: https://learn.cisecurity.org/20-controls-download



Internet Engineering Task Force (IETF) — E. Rescorla
Request for Comments: 8446 — Mozilla
Obsoletes: 5077, 5246, 6961 — August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8446.

Rescorla — Standards Track — [Page 1]

Source: https://datatracker.ietf.org/doc/rfc8446/

Changing Cyber Ecosystem

RF+IP=Mobility

IPv6 Only is the Goal

RF: 5G + BT + 6LoPAN

Mobile Networks (Space, Air, Land, Sea)

Machine to Machine (IoT, IIoT)

Wearable Technology

Industrial Control Systems

Supervisory Control and Data Acquisition

Critical Infrastructure Cross Sector Impact

Future…

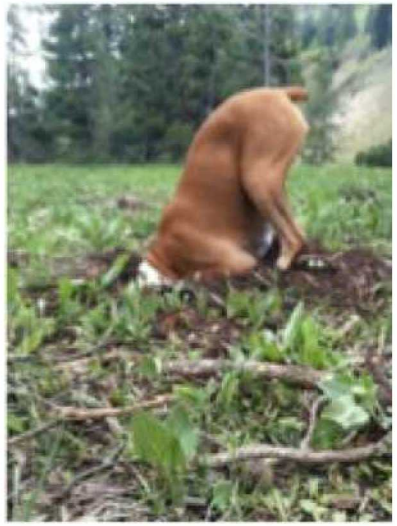
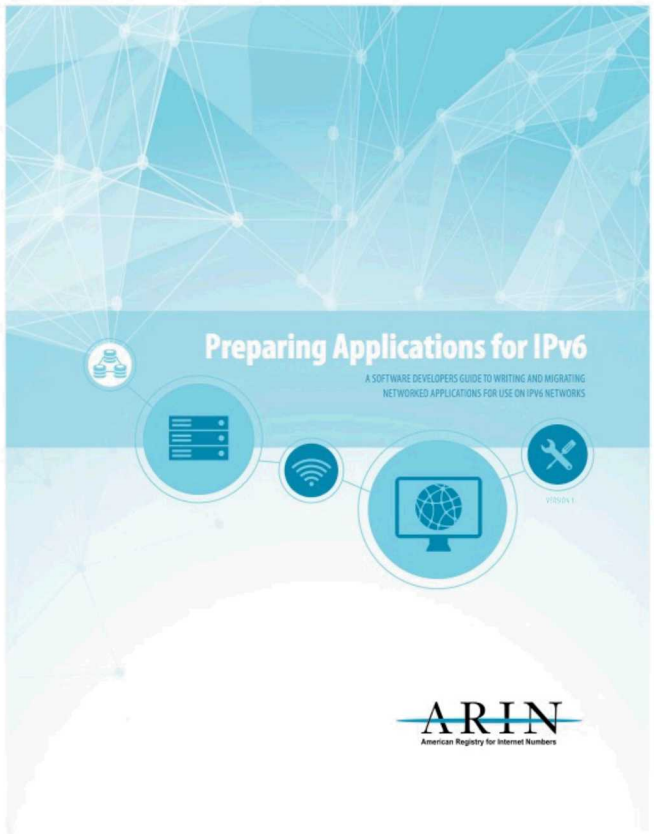


Photo Courtesy of Curtis Keliiaa

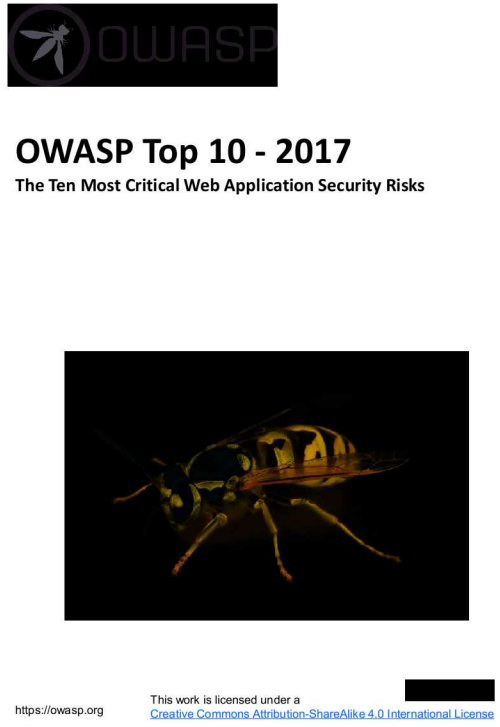
Is our cyber dog digging for clues, or just burying her head in the ground?

Secure Software



Source, July 2015: https://www.arin.net/knowledge/preparing_apps_for_v6.pdf

Source: https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf



Source: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Open Web Application Security Project

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies and other organizations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.

Application Security Test

Application Security (AppSec) enhances the confidentiality, integrity, and availability of information in application services. AppSec validated through risk-based activities reduces the time and cost to fix vulnerabilities; reduces vulnerabilities in production software; and increases the level of protection in the overall security posture. Protection is required when information is at rest, in transit, and in process. AppSec addresses the latter with application security types of test that may include:

Manual code review

Static application security testing (SAST) - used in two ways during development: Source code analysis for un-compiled code and configuration files; and for analysis of compiled byte or binary code

Dynamic application security testing (DAST) - used interactively with software execution in real time in two ways: Web application and application program interfaces (API); Non-web dynamic testing and fuzzing (manipulating protocols or data to observe results)

Interactive application security testing (IAST) - integrated static and dynamic vulnerability testing done through the instrumentation of running code. Three categorizations of IAST apply: Self-Testing to perform test driven from other test results (e.g. acceptance, sanity, functional); DAST-induced for additional DAST scanning to further assess an application for security vulnerabilities; and behavioral analysis to observe software as it runs

Mobile application security testing (MAST) - for testing mobile application security

Software composition analysis (SCA)

Code correction

Application wrapping technology to inject security functions after development

Threat Modeling

Keep Software Vulnerabilities Contained

Application Security Risk Level Categorization Example:

High:

Applications that support life safety or safety critical operations

Applications that process information with severe or catastrophic potential impact when confidentiality, integrity, or availability of information is compromised

Medium:

Applications that cross logical boundaries. For example, internal information is made available to the public internet, business partner, or government networks

Applications that process personally identifiable information (PII), export control information (ECI), or other sensitive information

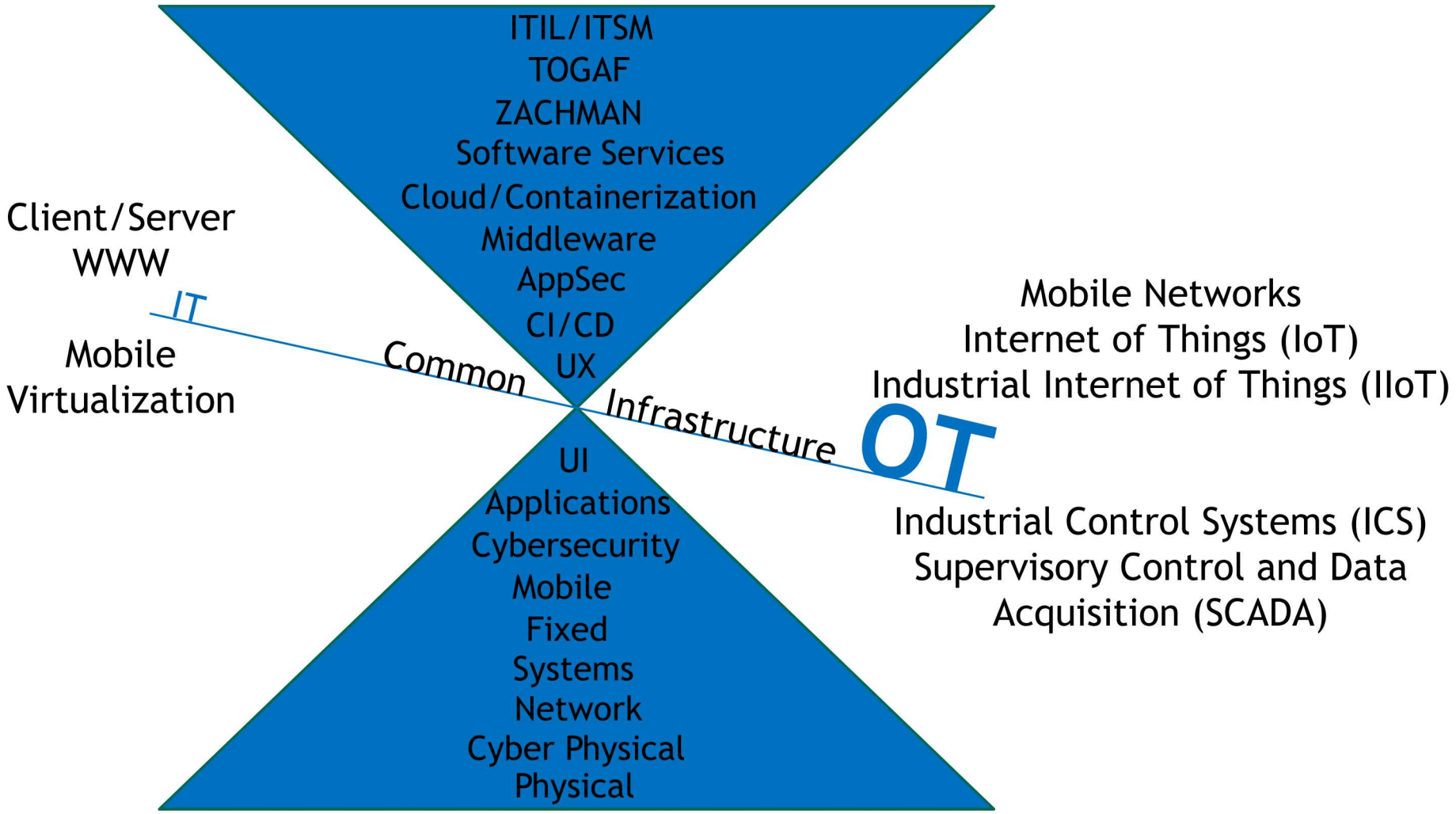
Applications that process information with serious potential impact when confidentiality, integrity, or availability of information is compromised

Low:
All other applications (e.g. inter-site or inter-domain)

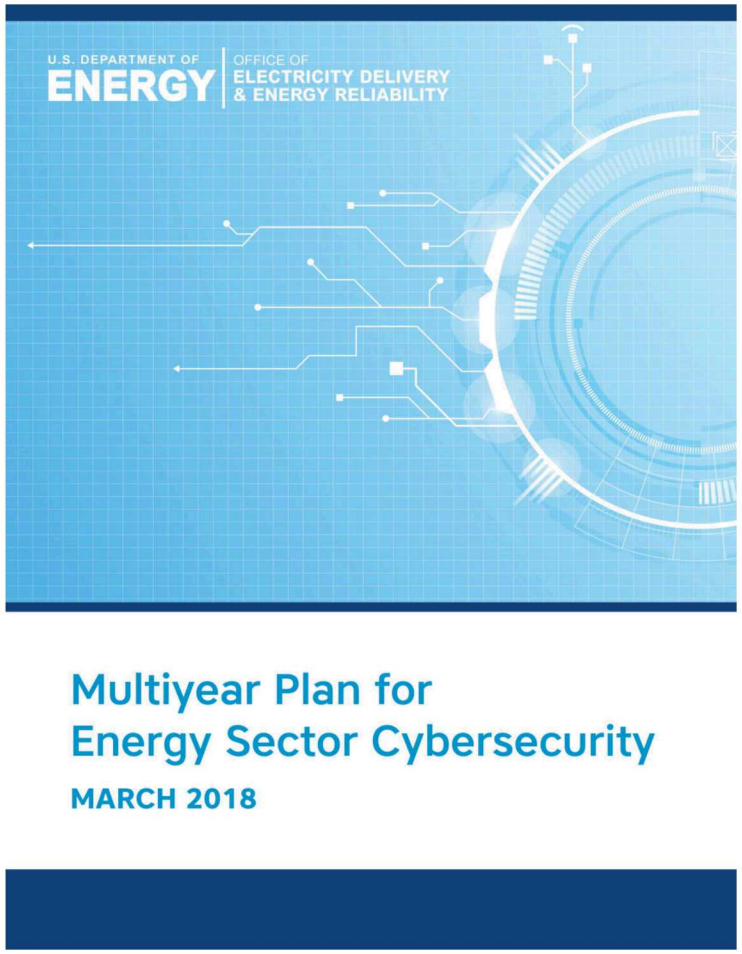
Reference: Standards for Security Categorization of Federal Information and Information Systems, FIPS 199: https://csrc.nist.gov/publications/detail/fips/199/final

Photo Courtesy of Curtis Keliiaa

Notional IT/OT Common Infrastructure Architecture Reference



Operational Technology Cybersecurity: Energy Example



Source:https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

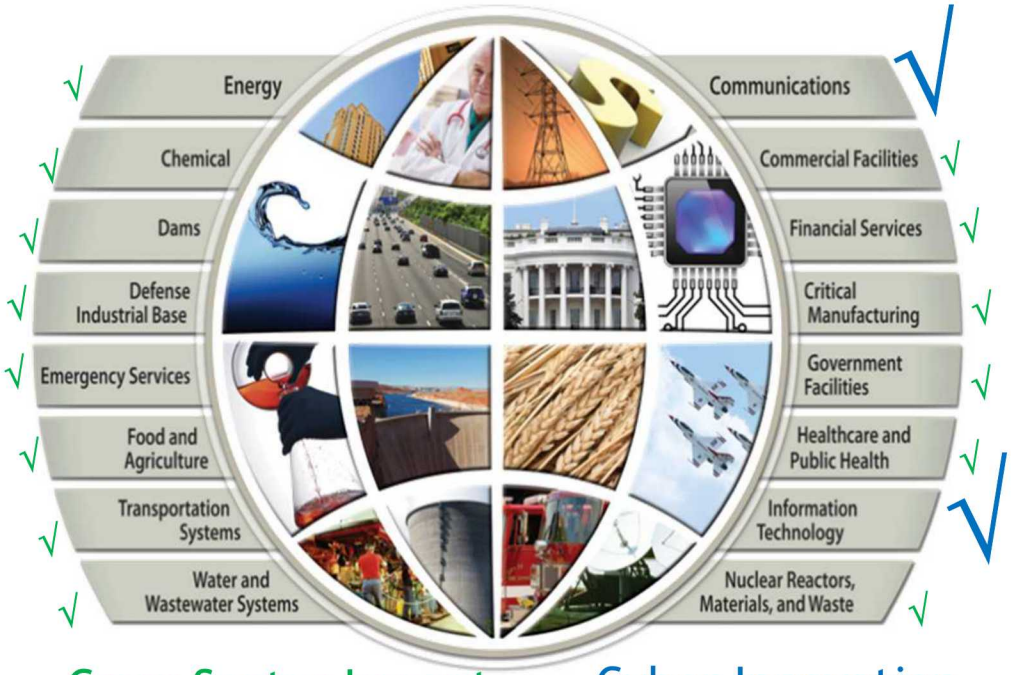
U.S. Department of Energy

CYBERSECURITY STRATEGY

2018-2020

Source: https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf

Critical Infrastructure

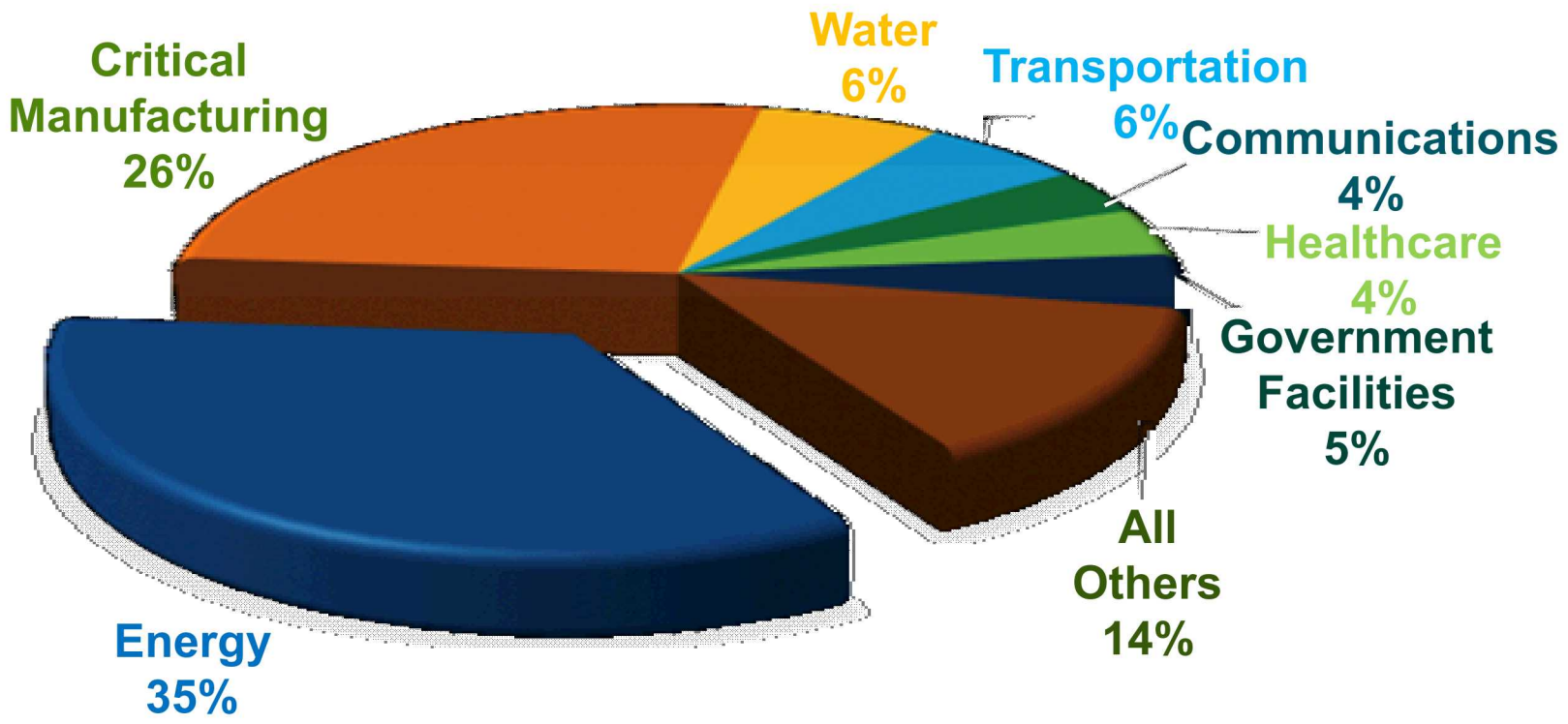


Source: Sandia National Laboratories: Resilient Infrastructure Systems

Reference: https://www.dhs.gov/critical-infrastructure-sectors

Information technology and communications innovations are driving advancements in smart infrastructure. The result is that government facilities, emergency services, energy, water, commercial facilities, and healthcare are becoming increasingly automated.

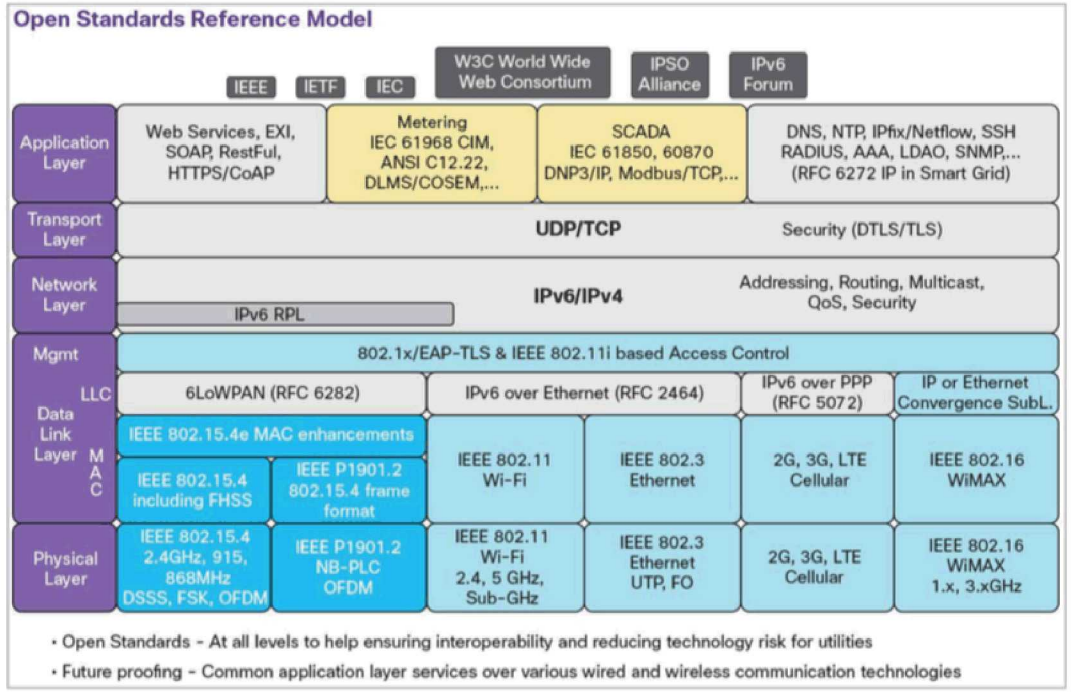
Critical Infrastructure Cybersecurity



Source: DOE 2018-2020 Multi-Year Plan for Energy Sector Cybersecurity
Figure 2. Critical Infrastructure Cyber Incidents Reported to DHS ICS-CERT (2013-2015)
https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

Standards Based Approach

1. Internet Engineering Task Force (IETF) Internet Protocol, version 6 (IPv6) leap ahead expansion
2. Institute of Electrical & Electronics Engineers (IEEE) radio frequency (RF) 5G standards for RF/IP design
3. International Electrotechnical Commission (IEC) Common Information Model (CIM) for complex systems



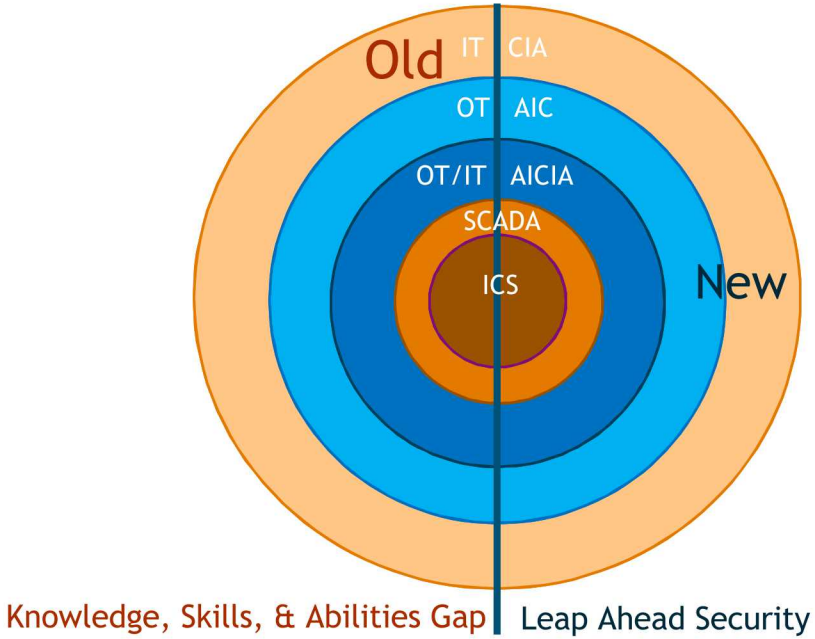
Source: https://www.cisco.com/c/en/us/solutions/industries/energy/external-utilities-smart-grid/field-area-network.html

Reference: http://www.iec.ch/smartgrid/standards/

Cybersecurity Principles

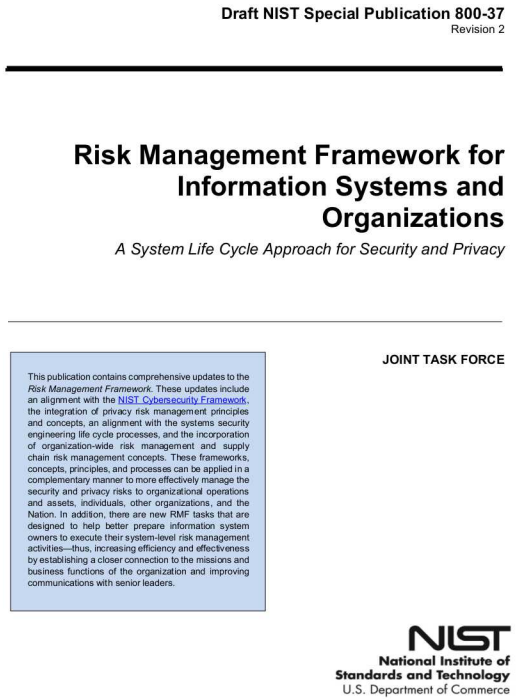
1. IT Cybersecurity: Confidentiality, Integrity, Availability
2. OT Cybersecurity: Availability, Integrity, Confidentiality (Energy Example)
3. Integrated OT/IT Availability Integrity [Confidentiality] Integrity Availability security model

Qualified Workforce
- Training & Certifications
- Professional Organizations
- Higher Education



Concept to Disposition: OT/IT Cyber Security, Physical Security, Resilience (CPR) Design Requirements

Multi-Domain Risk Management



Draft NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

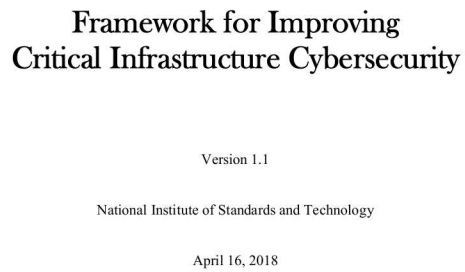
This publication contains comprehensive updates to the *Risk Management Framework*. These updates include an alignment with the NIST Cybersecurity Framework, the integration of privacy risk management principles and concepts, an alignment with the systems security engineering life cycle processes, and the incorporation of organization-wide risk management and supply chain risk management concepts. These frameworks, concepts, principles, and processes can be applied in a complementary manner to more effectively manage the security and privacy risks to organizational operations and assets, individuals, other organizations, and the Nation. In addition, there are new RMF tasks that are designed to help better prepare information system owners to execute their system-level risk management activities—thus, increasing efficiency and effectiveness by establishing a closer connection to the missions and business functions of the organization and improving communications with senior leaders.

JOINT TASK FORCE

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Source: https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-ipd.pdf

Prepare; Categorize; Select; Implement; Assess; Authorize; Monitor



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

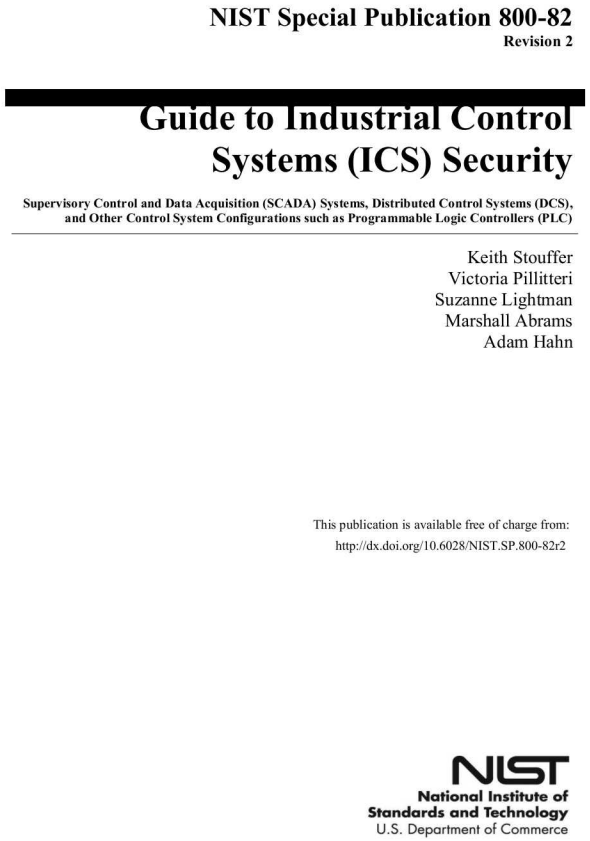
National Institute of Standards and Technology

April 16, 2018

Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Identify; Protect; Detect; Respond; Recover

NIST SP800-82, Revision 2



This May 2015 document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements.

Source: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

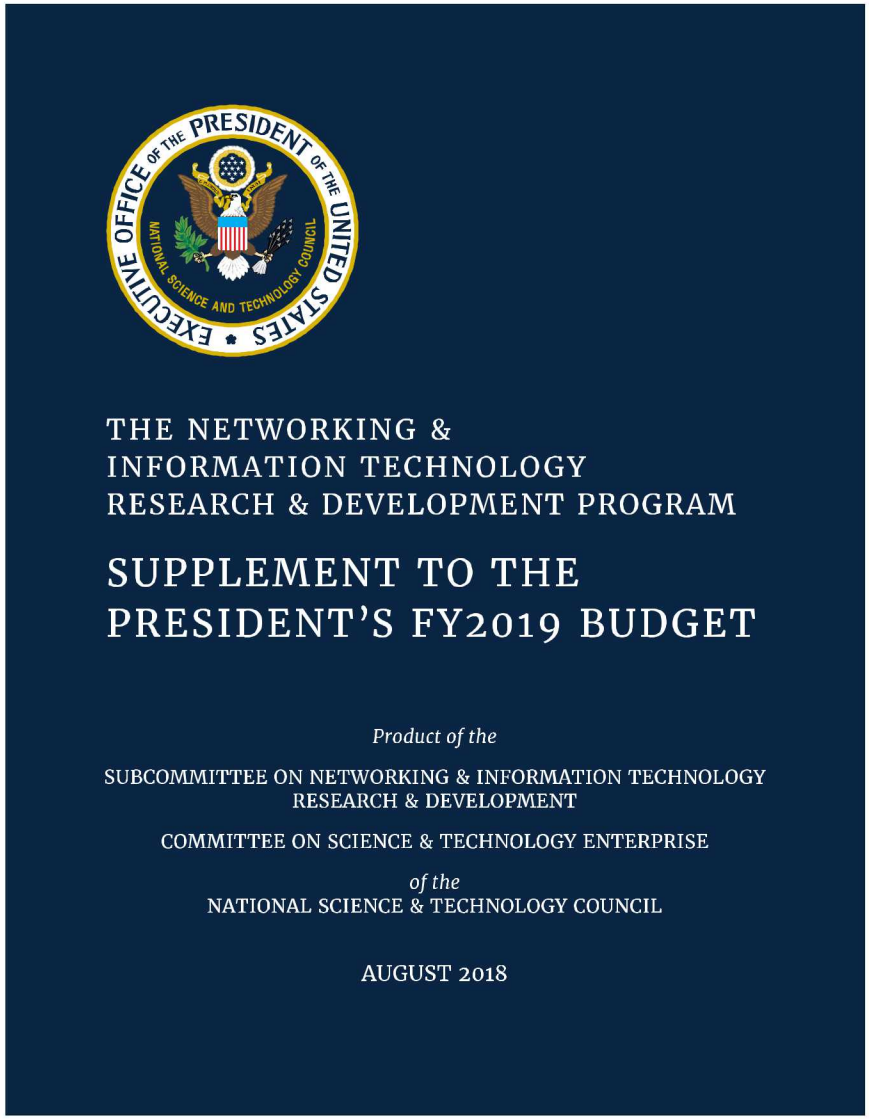
Smart Community Resilience

Community resilience means communities are safely and securely able to withstand a disruption of critical systems and services

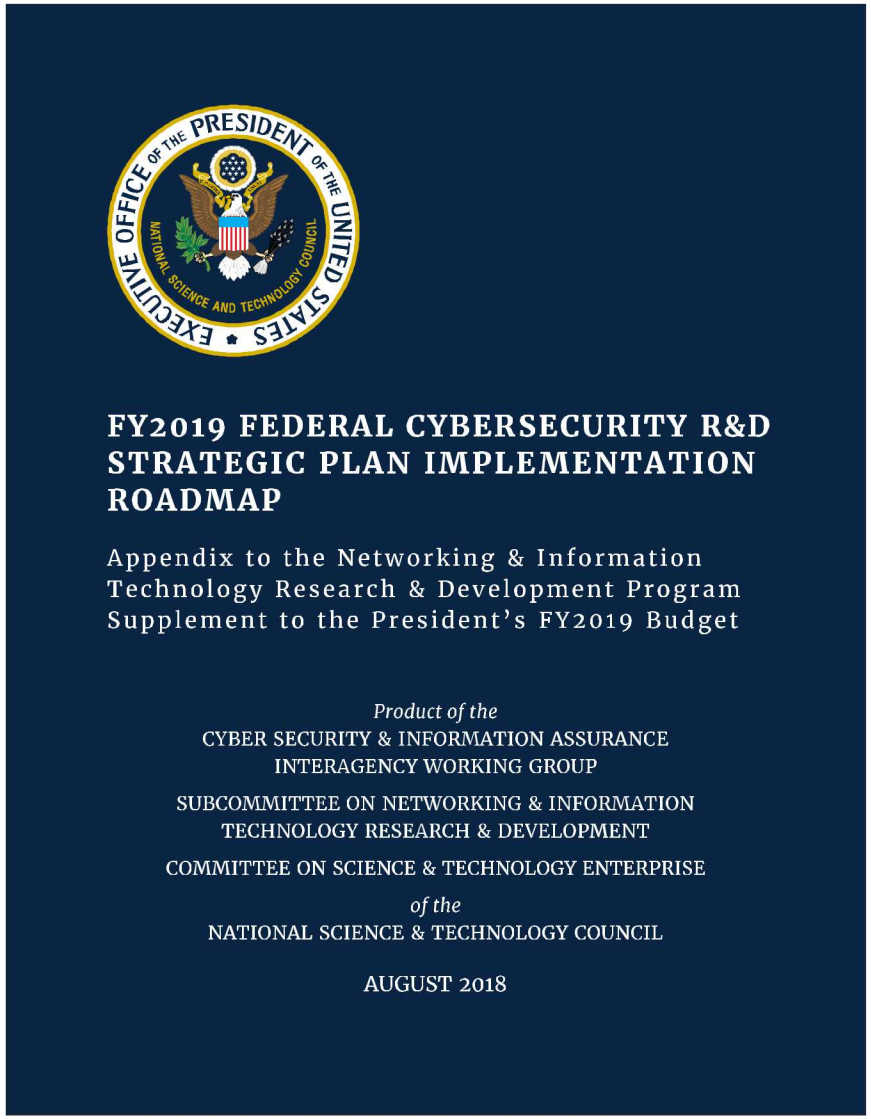
The Department of Homeland Security defines 16 national critical infrastructure sectors, which also apply to state, local, tribal, and territorial government interests and are a good starting point for identifying vital services for smart community resilience

Community concerns might include the availability of food, water and shelter during life safety events; continuity of government and businesses operations; or recovery from an IT disaster

Broadband Research and Development

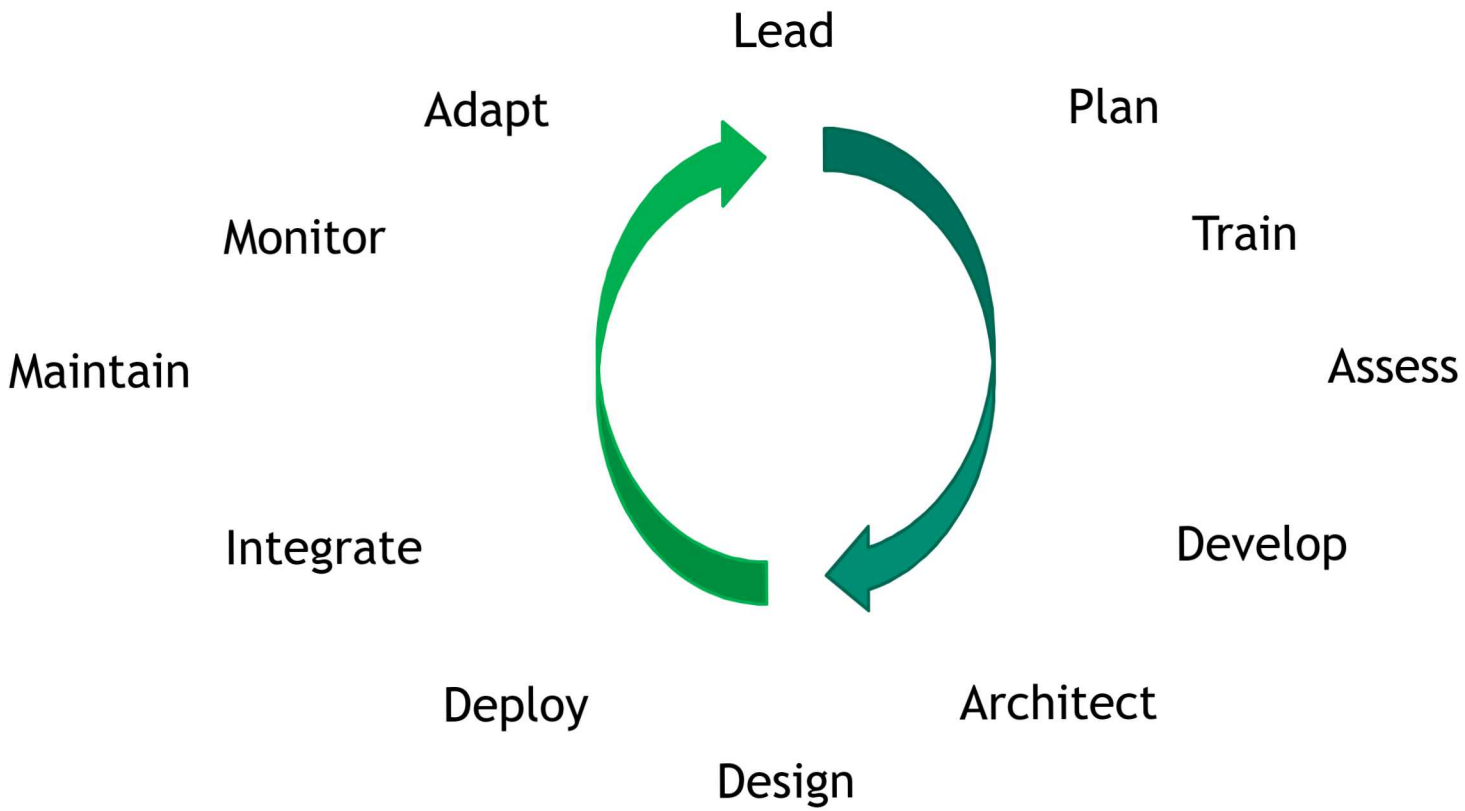


Source: https://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=92

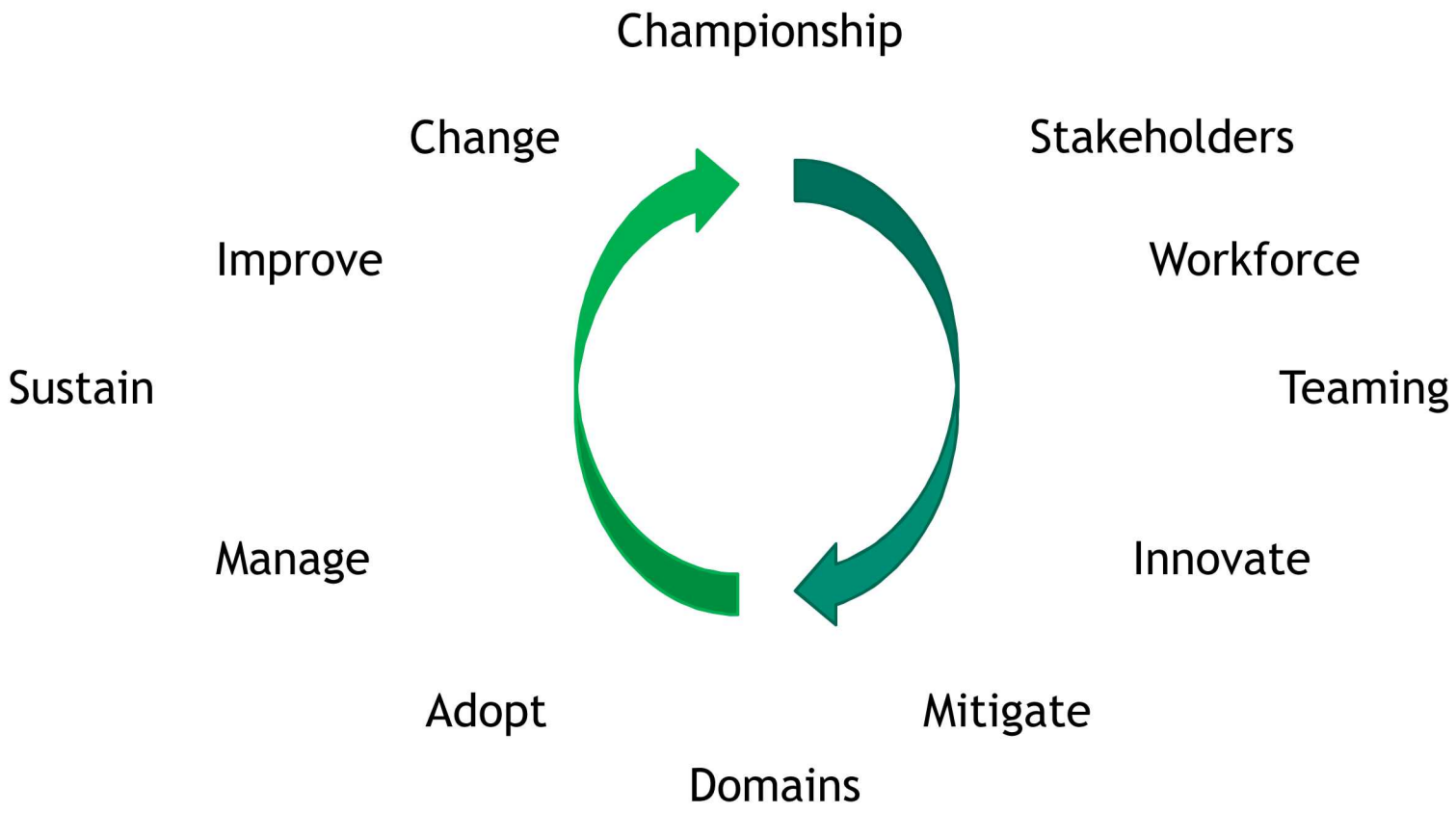


Source: https://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=91

What Can We Do About It?



How Can We Go About It?



Tying It All Together

Steps to Readiness include:

1. Inform executive leadership and gain leadership support
2. Identify what critical systems and services are currently in place
3. Identify how critical operations are done and gaps to be addressed
4. Gather key stakeholders for collaborative exercises and planning
5. Identify critical service OT/IT dependencies, for example workforce development pipeline, utilities, and supply chain
6. Identify likely threats that may endanger public safety and health or disrupt operations
7. Establish a smart infrastructure roadmap

Steps to Manage Risk include:

1. Partner for assistance and independent review
2. Conduct technical and operational risk assessments
3. Identify risk mitigations
4. Update OT and IT infrastructure to current standards
5. Develop OT/IT security
6. Require cybersecurity, physical security, and resilience in future design
7. Continually conduct best risk management practices for the highest protection posture

Key Points:

- Use updated standards and practices to build new systems & reduce risk
- Cybersecurity, Physical Security, and Resilience “CPR” design from the start
- Leap ahead smart infrastructure advantage with new technologies
- Executive championship for workforce development is required

Time is of the Essence

Video Courtesy of Curtis Keliiaa

The scale of change is vast, but what is most astounding is the rate of change!

References

Federal Communications Commission National Broadband Map, accessed 8/21/2018; https://broadbandmap.fcc.gov/#/area-summary

Networking and Information Technology Research and Development (NITRD) Program, Broadband Resource Guide, Draft: https://www.nitrd.gov/apps/broadband/

NITRD Program "NITRD Leads IT", Quarterly News Letter, July 2018 issue, https://www.nitrd.gov/pubs/newsletter/NITRD-Newsletter-07162018.pdf

NIST Special Publication 800-171 Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016, https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, August 2017, https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

IEEE 5G AND BEYOND TECHNOLOGY ROADMAP WHITE PAPER, , October 2017, https://5g.ieee.org/images/files/pdf/ieee-5g-roadmap-white-paper.pdf

NIST Special Publication 500-267Ar1 Revision 1, July 2018 Draft, https://www.nist.gov/sites/default/files/documents/2018/07/12/draft-nist-sp-500-267ar1.pdf

American Registry for Internet Numbers (ARIN), ARIN IPv4 Free Pool Reaches Zero, September 24, 2015, https://www.arin.net/vault/announcements/2015/20150924.html

The IPv6 Forum, http://www.ipv6forum.com

NIST Special Publication 500-267Ar1 Revision 1, NIST IPv6 Profile, https://www.nist.gov/sites/default/files/documents/2018/07/12/draft-nist-sp-500-267ar1.pdf

Internet Engineering Task Force (IETF), Network Working Group, Request for Comments (RFC): 4291 IP Version 6 Addressing Architecture, February 2006, https://tools.ietf.org/rfc/rfc4291.txt

Center for Internet Security (CIS), CIS Controls version 7, https://learn.cisecurity.org/20-controls-download

IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018, https://datatracker.ietf.org/doc/rfc8446/

ARIN Preparing Applications for IPv6, July 2015, https://www.arin.net/knowledge/preparing_apps_for_v6.pdf

SAFECode, Fundamental Practices for Secure Software Development, Third Edition, March 2018, https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf

The Open Web Application Security Project (OWASP), Top Ten-2017, The Ten Most Critical Web Application Security Risks, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Standards for Security Categorization of Federal Information and Information Systems, FIPS 199: https://csrc.nist.gov/publications/detail/fips/199/final

The Itil Open guide, http://www.itlibrary.org

Information Technology Service Management (ITSM) Tools, https://itsm.tools

The Open Group Architecture Framework (TOGAF) Version 9.2, http://www.opengroup.org/subjectareas/enterprise/togaf

John A. Zachman, The Zachman Framework for Enterprise Architecture, https://www.zachman.com/about-the-zachman-framework

U.S. Department of Energy, Multiyear Plan for Energy Sector Cybersecurity, March 2018, https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

U.S. Department of Energy, Cybersecurity Strategy 2018-2020, https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf

U.S. Department of Homeland Security, Critical Infrastructure Sectors, https://www.dhs.gov/critical-infrastructure-sectors

Smart Grid Field Area Networks, Open Standards Reference Model, https://www.cisco.com/c/en/us/solutions/industries/energy/external-utilities-smart-grid/field-area-network.html

International Electrotechnical Commission (IEC), Common Information Model (CIM), Smart Grid Standards, http://www.iec.ch/smartgrid/standards/

Draft NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations, May 2018, https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-ipd.pdf

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Guide to Industrial Control Systems (ICS) Security, Revision 2, May 2015, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

NITRD Program, FY2019 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap, August 2018, https://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=92

NITRD Program, Supplement To The President's FY2019 Budget, August 2018, https://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=91

Mahalo!, Questions Please

Curtis Keliiaa
(ISC)^2 Certified Information System Security Professional
IPv6 Forum Gold Certified Network Engineer
cmkelii@sandia.gov