National-Tribal Critical Infrastructure Protection: Collaboration for Extraordinary National Security Benefit SAND2020-5150

Curtis M. Keliiaa, CISSP

April 2020

This report examines a future forward concept of operations for extraordinary benefits in National-Tribal collaborative critical infrastructure protection. The Nations are faced with securing national critical infrastructures amid an ever-changing cyber-ecosystem. A comprehensive approach addresses an old/new digital dichotomy, whereby stakeholders can reduce complexity, risk, and cost, advance a capable workforce, and increase cyber disruption response and recovery capabilities. Preliminary risk and hazard assessments can be used to identify security design criteria that inform preemptive critical infrastructure mitigations. Data-centric security can be used to increase information asset protection as virtualization and software-defined infrastructure services advance automation. Multi-stakeholder collaboration is essential in the critical infrastructure protection national priority. A fulsome National-Tribal CIP solution is presented for improved measures to avoid, eliminate, or contain critical infrastructure vulnerabilities and reduce threat exposure.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

ABSTRACT

This paper examines national and tribal collaborative opportunities to get ahead of the critical infrastructure insecurity problem. Recommendations are viewed through the lens of the Sandia Labs Tribal Cyber-Energy initiative and national security projects. Recommendations include 1) Collaboratively address national priority and shared challenges to gain faster and better solutions to national priority problems on a smaller yet comprehensive American Indian and Alaskan Native sovereign single-point of authority scale 2) Utilize newer standards-based technologies to provide scalable, capable, and manageable solutions for greatly expanded and connected national critical infrastructures 3) Employ Cyber-Physical-Resilient design preliminary analysis to define concept-to-disposition design requirements for preemptive critical infrastructure risk mitigation and baked-in security; 4) Develop data-centric protection to provide increased information asset protection as data shifts from data-owner operated on-premises infrastructure to virtual service provider data-steward owned and operated off-premises infrastructure; and 5) Balance shared solutions with the National Institute of Science and Technology (NIST) Cybersecurity and Risk Management frameworks, and the System Security Engineering Guidelines.

As yet unallocated federal funding would support research, development, the timely application of National-Tribal critical infrastructure protection, and critical infrastructure Cyber disruption response and recovery with extraordinary mutual benefits for the foreseeable future.

The Critical Infrastructure Insecurity Problem: Rapid modernization and expansive connectivity are due to advances in Information and Communications Technologies that have sweeping cyber impact across all critical infrastructure sectors. Supervisory Control and Data Acquisition and Industrial Control Systems are particularly impacted as systems long separated from the Internet are now being connected and computerized. Virtualization and mobility create a Data Everywhere-User Anywhere paradigm that has evaporated the enterprise network perimeter. There are multi-front technological challenges at play, where long depended on technologies simply don't scale to current needs resulting in a digital dichotomy of competing old and new standards. New standards-based technologies scale but are not as well-known or as widely deployed, which leaves decision makers, stakeholders, and the workforce in a quandary, caught mid-stream between the technological past and the virtual future. Rapid and expansive cyber threat accompanies disruptive change in connectivity and computational dependencies. A lack of action will exacerbate the problem if new technologies roll out without baked-in security design.

The Risk: If National-Tribal CIP collaboration to design in security is not done, then an ongoing state of insufficient bolt-on security and elevated threat exposure will remain for years to come.

ACKNOWLEDGEMENTS

Acknowledgement and appreciation are extended to the Sandia National Laboratories Tribal Cyber-Energy team and project participants, the Sandia National Laboratories New Mexico Small Business Assistance (NMSBA) program and project participants, strategic partnership project customers including the membership of the Native American Telecom Association (NATA), the National Tribal Telecom Association (NTTA), the Sandia National laboratories Resilient Infrastructure Protection Technical Interdisciplinary Expertise (RIPTIDE) team, and the Cyber-Physical-Resilient (CPR) design team, all of whom contributed to the concepts and methodologies included herein.

Appreciation is extended to individual colleagues from who's contributions this work stands, these include Laurence Brown, Stan Atcitty, Sandra Begay, Ben Mar, Anya Castillo, Dylan Moriarty, Gepetta Billie, Angie Kelic, Barbara Jennings, Will Atkins, Ken Bernier, Ray Parks, Johnny Giere, Lita Suina, David Martinez, Ian Burres, Victor McLane, Brad Carvey, Patricia Crosno, Sam Olsen, and Ryan Birmingham.

This work comprises information garnered from several areas of work that the author supports: the Department of Energy's National Nuclear Security Administration - Advanced Computing Initiative; Department of Homeland Security - Continuous Diagnostics and Mitigation; Network and Information Technology Research and Development - Broadband Research Group; and the Sandia National Laboratories Tribal Cyber-Energy Initiative. These efforts motivate the National-Tribal CIP vision and inform much of the content herein.

The reader may observe a variety of styles within this literature review. This is done to preserve the value of content from various sources and contributors.

BIOGRAPHY

Curtis M. Keliiaa, Principal Investigator

Curtis is a senior staff member in Cyber Analysis R&D Solutions at Sandia National Laboratories (Sandia Labs) in Albuquerque New Mexico. His experience comprises many years in Information Technology (IT), communications, and cybersecurity. He led the Sandia Labs New Mexico IPv6 external facing services deployment and is the Cyber subject area lead for the Tribal Cyber-Energy critical infrastructure initiative. After delivering a Sandia Labs Business Continuity Plan and Business Impact Assessment in 2005, Curtis served on assignment in Washington, DC from 2006-2008, where he worked in the intelligence community on cyber risk mitigation. In 2015 he presented by invitation to the President's National Security Telecommunications Advisory Committee, Big Data Analysis Subcommittee regarding a 2010 High-Performance Computing (HPC) Cybersecurity Analysis R&D roadmap and served as the Red Storm HPC system Information System Security Officer. He has more recently presented "Protecting Information in Evolving Critical Infrastructure Services" at the 2019 $(ISC)^2$ Security Congress. He has initiated Cyber-Physical-Resilient design methodology, and currently provides Cloud security consultation to the Department of Homeland Security. Curtis is a Certified Information System Security Professional (CISSP), and an IPv6 Forum Gold Certified Engineer. His training and certification accomplishments over 40 years in industry and 30 years at Sandia Labs also include: Novell Certified Network Engineer (CNE), Microsoft Certified System Engineer (MCSE), Cisco Certified Network Professional (CCNP), SysAdmin Audit Network Security (SANS) GIAC Firewall Analyst, and Paraben Cell Phone Forensics certifications, Ham Radio License, and SANS Cloud Security, SANS Smartphone forensics and most recently SANS Industrial Control Systems Security training.

CONTENTS

1. Field of Work 11
    1.1. Tribal Cyber Work 11
    1.2. Tribal Energy Work 12
        1.2.1. DOE Office of Electricity's Energy Storage Tribal Energy 12
        1.2.2. DOE Office of Indian Energy Policy and Programs 13
    1.3. Tribal Cyber-Energy Work 14
    1.4. National-Tribal CIP Research and Development 15
    1.5. Education and Workforce Development 16
    1.6. Critical Infrastructure Digital Transformation 18
    1.7. Risks, Attack Surface, and Mitigations 18
    1.8. Sandia Labs World-Class Science and Engineering 19
    1.9. Project Costs and Estimates 21
    1.10. Critical Infrastructure Protection - Extraordinary Benefits 22
2. The Power of Collaboration 23
    2.1. U. S. Government and Tribal Collaboration 23
        2.1.1. Department of Interior 24
        2.1.2. DOI Office of Chief Information Officer – Telecommunications 26
            2.1.2.1. Voice Services 26
            2.1.2.2. Network Services 26
            2.1.2.3. Radio Communications & Spectrum Services 27
        2.1.3. Interdepartment Radio Advisory Committee (IRAC): 28
        2.1.4. FCC Initiatives and Findings 29
            2.1.4.1. Recommendations for Executive Action 30
        2.1.5. NTIA Broadband Programs across the United States: 31
            2.1.5.1. NTIA 2.5 GHz Rural Tribal Window 32
    2.2. U.S. Government Adoption of IPv6 32
3. Cyber Infrastructure Modernization 33
    3.1. Standards Based Technical Investments 33
        3.1.1. Internet Protocol 33
        3.1.2. Radio Frequency 33
        3.1.3. IPv6 and 5G NR 33
        3.1.4. Virtual Technologies 36
        3.1.5. Data Center and Environmental Controls 37
        3.1.6. Cloud Services 38
    3.2. Wide Area Broadband Network Design 39
        3.2.1. Secure and Resilient Broadband Big Picture 39

3.3. Design Assurance 41
3.3.1. Planning & Design Phase 41
3.3.2. Design & Implementation Phase 41
3.3.3. Review/Post-Implementation Phase 41
3.4. Physical Security Policies and Access Control Procedures 41
3.4.1. Enterprise Information Security Policy 42
3.4.2. Issue-Specific Security Policy 43
3.4.3. System-Specific Security Policy 43
3.4.3.1. ISO 2700 Series 43
3.5. NIST Security Models 44
3.5.1. Securing Local Area Networks(s) / Physical Network Settings 45
3.5.2. Securing Wide Area Networks / Wireless Access Settings 47
3.5.3. Internal Monitoring Capabilities 49
3.5.3.1. Log Review 49
3.5.3.2. Ruleset Review 49
3.5.3.3. System Configuration Review 49
3.5.3.4. Periodic Penetration Tests/Vulnerability Assessments from Independent Companies/Organizations 50
3.6. Training 51
4. Risk Management 53
4.1. The NIST Special Publication 800-37, Revision 2 53
4.2. NIST Special Publication 800-160, Volume 2 55
4.3. Data Centric Protection Approach 57
4.4. Cyber Risk Assessments 60
4.4.1. Administrative Risk 60
4.4.2. Technical Risk 60
4.4.3. Operational Risk 60
4.4.4. Physical Risk 60
4.5. Design Assessments 60
4.5.1. Physical Risk Assessments 60
4.5.2. Hazard Assessments 60
4.5.2.1. Natural Hazards 61
4.5.2.2. Manmade Hazards 61
4.5.2.3. Technological Hazards 61
4.6. Operational Security 61
4.7. Cyber Physical Resilient Design 63
4.8. NIST Cyber Security Framework 63

5. Response and Recovery from Cyber Disruptive Events 66
5.1. Identity Credential and Access Management 66
5.1.1. Identity Management 66
5.1.2. Credential Management 66
5.1.3. Access Management 66
5.2. Cloud Security Practices 66
5.2.1. Least Privilege 66
5.2.2. Service Accounts 67
5.2.3. Auditing 67
5.2.4. Policy Management 67
5.2.5. Centralize Identity Management 67
5.2.6. Connected Tenants 67
5.2.7. Single Sign-On 68
5.2.8. Conditional Access 68
5.2.9. Password Management 68
5.2.10. Multi-factor Authentication 68
5.2.11. Role-Based Access Control 68
5.2.12. Privileged Accounts 68
5.2.13. Monitoring 69
5.2.14. Identity Stores 69
5.2.15. Federation Capabilities 69
5.2.16. Password Policy 69
5.2.17. Temporal Roles 69
5.3. ICAM in the Cloud 69
5.3.1. User Management 70
5.3.2. Authentication Management 70
5.3.3. Authorization Management 70
5.3.4. Access Management 70
5.3.5. Data Management 70
5.3.6. Monitoring and Auditing 70
5.3.7. Application Program Interfaces 71
5.4. Cyber Relevant Time 71
5.5. Cybersecurity 72
5.5.1. Operational Support Systems 73
5.6. Adoption of the NIST Cyber Security Framework 73
5.6.1. Implementation Tiers 73
5.6.1.1. Tier 1: Partial 73

5.6.1.2. Tier 2: Risk Informed 73
5.6.1.3. Tier 3: Repeatable 74
5.6.1.4. Tier 4: Adaptive 74
5.6.2. Cloud CRT and CSF Adaptation 74
5.6.2.1. Cloud: Identify 75
5.6.2.2. Cloud: Protect 75
5.6.2.3. Cloud: Detect 75
5.6.2.4. Cloud: Respond 75
5.6.2.5. Cloud: Recover 76
6. Design Recomendations 77
6.1. Design Planning 77
6.1.1. Internet Protocol 77
6.1.2. Radio Frequency and Optical Communications 78
6.1.3. Data Center Virtualization 78
7. Industrial Control System Security 79
7.1. The NIST Special Publication 800-82, Revision 2 79
7.2. The New Technological Paradigm 79
8. Integrated Emergency, Continuity, and Cyber Response and Recovery 80
9. Key Takeaways 85

LIST OF FIGURES

Figure 1. Emergency Management Tabletop Exercise 12
Figure 2. Sandia Labs Tribal Cyber-Energy Team Visit to Blue Lake Rancheria Microgrid 14
Figure 3. Multiphase Fluid Property (Contact Angle) Micro-CT Scan Calculation 16
Figure 4. Consortium Enabling Cybersecurity Opportunities & Research 17
Figure 5. Consortium for Integrating Energy Systems in Engineering & Science Education 17
Figure 6. Advanced Manufacturing Initiative Network led by the American Indian Higher Education Consortium 17
Figure 7. Quantum State Illustration 19
Figure 8. CARVR Idea Lab 20
Figure 9. SlyCat Table View 20
Figure 10. SlyCat Time Series View 21
Figure 11. Department of Interior Hierarchy Structure 24
Figure 12. Bureau of Indian Affairs, "About Us" 25
Figure 13. BIA Regional areas in continental United States excluding Alaska/Hawaii 26
Figure 14. Chart for Effective Telecommunications Architecture 28
Figure 15. IRAC Members 29

Figure 16. NITRD: Broadband Resource Guide 39
Figure 17. DHS Critical Infrastructure Sectors 40
Figure 18. Energy Field Area Network Common Reference Architecture 40
Figure 19. ISO 27002 Information Security Management Methodology 44
Figure 20. Security Perimeter and Defense in Depth [excerpted] 45
Figure 21. Physical/Logical Topologies 46
Figure 22. Demilitarized Zone Example 48
Figure 23. 100-Years Perspective of the Digital Dichotomy 52
Figure 24. Internet Protocol Threat Reduction toward a Single Standard 52
Figure 25. NIST RMF Organization-Wide Risk Management Approach 53
Figure 26. Risk Management Framework Tasks 54
Figure 27. NIST RMF Conceptual View of a System and Environment of Operation 54
Figure 28. NIST SP800-160, v2 System Life Cycle Processes and Stages 55
Figure 29. Cyber Resiliency Techniques and Implementation Approaches 56
Figure 30. Cyber Peanut Game Board - Functions, Roles, and Responsibilities 58
Figure 31. Radio and Telecommunications Diagram, DOE-HDBK-1233-2019 62
Figure 32. Attacker vs. Defender Timeline 71
Figure 33. CPR-CSF Mapping to the Changing Cyber-Ecosystem 72
Figure 34. NIST CSF Core Structure 73
Figure 35. IPv4 Address Exhaustion 9-24-2015 77
Figure 36. Primary IPv4 IPv6 Differences 78
Figure 37. Integrated Emergency and Cyber Response and Recovery: Command Structure 81
Figure 38. Integrated Emergency and Cyber Response and Recovery: Operations 82

LIST OF TABLES

Table 1. Example Information and Communications Work Breakout 11
Table 2. High-Level Risks, Attack Surface, and Mitigation 19
Table 3. National-Tribal CIP Estimated Scale, Cost, and Value 21
Table 4. Non-Interoperable Technology Standards 37
Table 5. Cloud Service Terms and Definitions 38
Table 6. Data Centric Brainstorming Example Results 59
Table 7. Overview of NIST CSF Functions 65
Table 8. Cyber Relevant Time: Buyer/Supplier Roles and Cybersecurity Functions 72

EXECUTIVE SUMMARY

Sandia National Laboratories (Sandia Labs) is a premier Department of Energy (DOE) science and engineering national security facility. Sandia Labs primary site is in Albuquerque New Mexico, a rural state with significant unserved or underserved broadband service areas and populations. Albuquerque is known as a tribal hub because of Department of Interior (DOI), Bureau of Indian Affairs (BIA), and Bureau of Indian Education (BIE) presence and a significant Tribal/Pueblo residency. The intersection of the federal, tribal, and national security capabilities is relevant both regionally and nationally. Accordingly, Sandia Lab's Tribal Cyber-Energy team proposes a National-Tribal critical infrastructure protection (CIP) strategy for extraordinary benefit on the national CIP scale.

American Indian and Alaska Native Tribal Governments exercise single-point of authority over their critical infrastructure sectors. National and tribal concerns and goals converge with rural broadband expansion and critical infrastructure modernization. For example, some tribes lead in energy development and preparedness. Sandia Lab's national and tribal objective advisory is central to these concerns. Tribal Cyber-Energy project successes include:

- Emergency Management Modernization: Emergency Communications, Preparedness, and Security in the Arizona, Nevada, and California region
- Distributed Energy Resource Modernization: Energy Security in California, New Mexico, and Florida
- Cyber Infrastructure Modernization: Information Technology (IT) and Communications technical investments and security for the Native American Telecom Association (NATA) membership
- Risk Management: Cyber Security Framework and Recovery from Cyber Disruptive Events
- Design Technical Assistance: Regional Pueblo/Tribal broadband network design guidance

National-tribal work reveals that bridging the digital divide is concurrent with bridging the energy divide. Therefore, collaboration becomes essential when innovation, safety, and security are levied in a rapidly changing cyber-ecosystem. In addition, the digital and energy divides coincide with a digital dichotomy of legacy standards being displaced by current standards. The digital dichotomy is evident where current scalable standards are not backward compatible with long deployed but exhausted legacy standards. Key drivers for new standards deployment include:

- Scalability to serve the vast growth in broadband connectivity of fixed and mobile devices and sensors
- Capability to serve expanded software defined and/or virtual services
- Manageability of integrated IT, operational technology (OT), and Internet of Things (IoT) in modernized Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

The digital dichotomy presents challenges for all stakeholders that must be informed of the risks of continued use of legacy technologies that can't scale; and conversely, transitioning to current, and in some cases still developing technologies that pose new capabilities and risks. Old versus new technical investment choices place decision makers in a catch-22 "risk if you do and risk if you don't" scenario. Therefore, one must consider an informed and secure migration to scalable standards-based technologies to reduce complexity, risk, and cost. Subsequently, workforce knowledge, skills, and abilities (KSA) will also need to advance with large scale technological change.

A risk of continued insufficient bolt-on security exists if inaction delays the secure deployment of standards-based critical infrastructure modernization. Alternatively, innovation in unserved and underserved areas and new digital service development presents an unprecedented opportunity to "bake-in" security. New digital services can be an opportunity to modernize, secure, and set positive control in the national-tribal critical infrastructure solution space.

Federal funds investment will support a comprehensive security model for all critical infrastructure stakeholders. Opportunities include: 1) Collaboratively gain superior solutions to national priority and shared challenges on a smaller yet comprehensive American Indian and Alaskan Native sovereign single-point of authority scale 2) Utilize newer standards-based technologies to provide scalable solutions for greatly expanded and connected critical infrastructure 3) Employ Cyber-Physical-Resilient design preliminary analysis to define concept-to-disposition design criteria for preemptive critical infrastructure risk mitigations and baked-in security; 4) Develop data-centric protection to provide increased information asset protection as data shifts from data-owner operated on-premises (On-Prem) infrastructure to virtual service provider data-steward owned and operated off-premises (Off-Prem) infrastructure; and 5) Balance shared solutions with the National Institute of Science and Technology (NIST) Cybersecurity and Risk Management frameworks, and System Security Engineering Guidelines. Sandia Labs Tribal Cyber-Energy interdisciplinary teaming and objective advisory stands ready to facilitate extraordinary CIP benefits.

1. FIELD OF WORK

Sandia Labs has a proven history of work with national critical infrastructure security and American Indian and Alaskan Native (AI/AN) Tribal Government stakeholders. *There are 574 Indian Nations (variously called tribes, nations, bands, pueblos, communities and native villages) in the United States. These Indian Nations, recognized by federal policies as American Indian and Alaska Native Tribal Governments, are referenced formally throughout the document. Tribal Government stakeholders are representative of the many critical infrastructure stakeholders that National-Tribal CIP work seeks to assist. American Indian and Alaska Native or Native American terms may be used interchangeably as a collective reference to tribal communities and peoples unless Tribal affiliation is specifically stated. Laurence Brown, a Navajo Nation Citizen, leads the Tribal Cyber-Energy team by providing guidance for Tribal Government interaction, protocol and communications as Sandia Lab's Tribal Government Relations Officer. Laurence's vision and leadership has enabled this field of work.*

The National-Tribal CIP composite national security, economic, technological, and socioeconomic advancements support critical infrastructure resilience in alignment with secure national broadband expansion and computational modernization. Areas of innovation and increasing risk include the IoT, Mobile IoT, and Industrial IoT, which are in large part considered as modernized critical infrastructure instrumentation.

Our staff members are uniquely suited to understand National-Tribal CIP as American Indian and Native Hawaiian national security subject matter experts. *The Tribal Cyber-Energy team has developed trust with American Indian Tribal Government stakeholders over many years. AI/AN communities are each unique and American Indian critical infrastructure leaders are comfortable working with Sandia Lab's native professionals because of the personal and professional understanding of Indian Country concerns and passion that team members possess.*

1.1. Tribal Cyber Work

The Tribal Cyber team is staffed by Sandia Labs experts in Cyber critical infrastructure and protection, Embedded Systems Engineering, and Data Analytics. Tribal Cyber national, regional, and New Mexico Small Business Assistance (NMSBA) and strategic partnership project (SPP) work addresses the unique needs of each AI/AN Tribal Government stakeholder customer. The team typically provides objective advisory in the following subject areas:

- Cyber Infrastructure Modernization - Guidance for standards-based technical investments and resilience
- Risk Management - Cyber Security Framework alignment to respond and recover from cyber disruptive events
- Design Technical Assistance - Broadband network and security design considerations

Table 1. Example Information and Communications Work Breakout

Task	Desired Outcome	Deliverable
Cyber Infrastructure Modernization	ICT Technical Investments	Guidance for Technical Investments and Resilience
Risk Management	Cybersecurity	Cybersecurity Framework Alignment
Design Technical Assistance	Regional Broadband Network Security	Regional Broadband Network and Security Design Recommendations
Recommendations and Reporting	Secure and Resilient Regional Broadband	Written Analysis and Assessment Results

Curtis Keliiaa, Washoe Tribal Citizen, Cherokee and Native Hawaiian, and Ben Mar, Cherokee, lead Tribal Cyber projects. Curtis is a veteran IT, Communications and Cybersecurity professional. Ben is an Embedded Systems and Cybersecurity engineer.

NMSBA projects have been conducted with the Mescalero Apache Telecom, Inc., the Sacred Wind Telecommunications, Inc., and the Pueblo de Cochiti High Water Mark, Inc. The High Water Mark project also addressed education broadband access and security in association with Santa Fe Indian School (SFIS) and the Middle Rio Grande Tribal/Pueblo Consortium (MRGTPC). These companies are New Mexico resident small for profit businesses.

NMSBA and SPP project workflow starts with relationship development and trust building, followed by cooperative statement of work definition, AI/AN tribal funds application and grant award, and execution of deliverables within the statement of work. Infrastructure resilience, cybersecurity, internet protocol (IP), radio frequency (RF) spectrum, and design assurance are areas that the Tribal-Cyber team excels in to provide technical assistance to tribes.

Sandia Labs Information Design Assurance Red Team (IDART) is another important set of disciplines that the team brings to Tribal Cyber analysis. IDART is considered an integral practice that the Cyber-Physical-Resilient (CPR) design team uses to assess emergent and secure information, communications, and virtual technologies. IDART and CPR design provide critical system security advantage gained through preliminary assessments with the goal of preemptive critical infrastructure mitigations.

Sandia Labs objective advisory is empowered by interdisciplinary teaming. For example, Tribal-Cyber staff support federal Cloud computing security and the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program. CDM is intended to provide federal departments and agencies with commercial off-the-shelf capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Similar adjudication would be very valuable to AI/AN critical infrastructure stakeholders to resolve common concerns.

The Tribal-Cyber team led a 2014-15 SPP for the Fort Mojave Indian Tribe Emergency Management Department. The focus of the SPP was Emergency Management modernization and resilience with regard to multiple stakeholders in Arizona, Nevada, and California. The project included FirstNet, Tribal Police, and Tribal Telecom stakeholder participants. The project was conducted by a Resilient Infrastructure Protection Technical Interdisciplinary Expertise (RIPTIDE) team. RIPTIDE comprised Sandia Labs world-class resilient infrastructure, emergency communications, and IT and RF Communications expertise. The project successfully delivered technical assessments for modernization, and a resilient infrastructure path forward, including a full scope tabletop exercise for multiple Public Safety Answering Points (PSAP).

Photo Courtesy Randy Montoya, Sandia National Laboratories

Figure 1. Emergency Management Tabletop Exercise

1.2. Tribal Energy Work

The Tribal Energy team is staffed by Sandia Labs interdisciplinary experts in Cyber-Energy research and development (R&D), Energy Storage and Power Electronics, Indian Energy, and Data Analytics. Examples of Tribal Cyber-Energy work are discussed below.

1.2.1. DOE Office of Electricity's Energy Storage Tribal Energy

The DOE Energy Storage Program leads a world-wide effort in addressing energy issues through energy storage R&D for grid-tied and off-grid systems throughout the nation including tribal lands. Dr. Stan Atcitty, who is a citizen of the Navajo Nation and electrical engineer, leads the Energy Storage Power Electronics and Tribal Energy Storage programs. He has over 20 years of experience in energy related R&D and has significant understanding of materials to systems energy research. The following provides a brief summary of Tribal Energy Storage projects:

- Energy Storage Benefits to the Alaskan Village of Levelock – There are over 70 enrolled tribal members at the Alaskan Village of Levelock residing on 7,744 acres of tribal land. The tribe currently has three diesel

generators that provide 100% of the electricity. Due to high fuel cost, high electricity cost and high emissions from the generators, the tribe is embarking on installing a microgrid with energy storage. The microgrid will consist of a new diesel generator, battery storage, and power conversion system. Sandia Labs will be providing pre-microgrid baseline analysis of load profile, resiliency, and cost of operation. In addition, Sandia Labs will provide post-microgrid installation analysis of battery performance, fuel usage, load profile, heat output, cost of operation, and resiliency.

- Energy Storage Benefits for the Navajo Nation – The Navajo Nation has over 350,000 tribal members and a reservation approximately the size of West Virginia (~17.5M acres). Currently, there are over 18,000 residents without electricity due to the expense of installing electrical infrastructure. The Navajo Tribal Utility Authority (NTUA), established in 1959, provides electrical, water, and natural gas services. To electrify the remote homes, NTUA is installing photovoltaic (PV) and/or wind generators with energy storage turn-key systems. These systems use traditional lead acid batteries and they have proven dependability but come at a cost with replacing them every 3-5 years. Urban Electric Power and Sandia will be installing a new battery technology, the zinc manganese oxide batteries. Once installed, the performance of these batteries will be compared to the lead acid batteries.
- Energy Storage Benefits to the Picuris Pueblo – The Picuris Pueblo has approximately 300 enrolled members and their reservation is small at 256 acres located in the Sangre de Cristo Mountains, in northern New Mexico. The tribe currently has a 1MW PV connected to their local electrical utility system. The tribe is considering the deployment of a microgrid with energy storage due to the high energy cost of electricity. Sandia Labs will be evaluating electrical service scenarios and resiliency solutions for large scale energy storage and PV designs.
- Energy Storage Benefits for San Carlos Apache Tribe – The San Carlos Apache Tribe is in the southeastern part of Arizona on a reservation slightly larger than Delaware (1.8M acres). They have approximately 17,000 tribal members. The tribe has unreliable power with 100 power outages per year and high energy cost especially during the monsoon season. They have some renewable community projects underway and one of which, is a design for a 2-3MW PV plant to be co-located with the San Carlos Healthcare Hospital. There is consideration for PV and energy storage integration. Sandia Labs will be providing cost saving estimates for net energy metering customers using behind-the-meter energy storage system.
- Energy Storage Benefits to Seminole Tribe of Florida – There are five Seminole Indian Reservations in Florida and a tribal trust land. They have 4,244 tribal members and their reservation spans nearly 100,000 acres of land within the borders of Florida. The tribe experiences grid instabilities caused by weather-related events. They have 100 outages per year and utilize 20 hours per week using diesel generation. They are exercising energy independence by installing PV and energy storage system across eight facilities. Sandia Labs is providing technical assistance in the request for proposal (RFP) development and vendor selection and review commission plan.

1.2.2. DOE Office of Indian Energy Policy and Programs

The DOE Office of Indian Energy Program funds a variety of projects to assist American Indian tribes and Alaska Native villages focused on energy development, energy cost reduction, capacity building, and electrification of tribal lands and homes. *Sandra Begay, a member of the Navajo Nation and a civil and structural engineer, has led Sandia Lab's technical efforts in assisting American Indian tribes with their renewable energy developments for over 17 years*. The following provides examples of Sandia Lab's contributions.

- Facilitation of strategic energy planning
- Technical assistance
- College student internship program 2002-2019 – The Office of Indian Energy provides American Indian students opportunities for current full-time undergraduate and graduate students who are familiar with American Indian culture and tribal issues. This program is extremely successful in that since 2002, 40 undergraduate and graduate interns have participated in the program, of which 64% were female interns. In total, 21 different tribal affiliations, 19 different majors were represented and 15% of the interns were hired as full- time employees (FTEs) or Sandia Labs contractors.

1.3. Tribal Cyber-Energy Work

The Tribal Cyber-Energy team combines the expertise of Cyber and Energy work, enabling a concentration for Cyber-Energy critical infrastructure modernization and protection. This work has led to understanding the impact that IT and Communications sector innovation is having in Energy and across other critical infrastructure sectors.

Sandia Labs strength is being able to draw from an array of world-class science and engineering disciplines to provide objective advisory to national and tribal stakeholders. The Tribal Cyber-Energy team leverages Sandia Labs deep science and engineering capabilities in our work with federal agencies and AI/AN Tribal Government stakeholders. Teaming in this way brings the right experts to the table for sets of very complex challenges.

Energy challenges include aging infrastructure and hardening distributed energy systems for resilience. CIP work addresses additional concerns including facilities and community planning. This whole community approach results in sustainable solutions, it's not just about technology. *Gepetta Billie, who is a citizen of the Navajo Nation provides facility and community planning expertise.*

Tribes are leading in modernized critical infrastructure development. An outstanding example is the Blue Lake Rancheria tribe in northern California. The original resiliency intent was to be a safe zone for tsunami events, but the value has been proven resilience through California's rolling blackouts due to wildfires. Illustrated below is a Tribal Cyber-Energy team visit to the Blue Lake Rancheria microgrid[1] installation in association with 2018 work for the DOE Office of Indian Energy Program. Pictured left to right are: *Gepetta Billie, Curtis Keliiaa, Stan Atcitty, Laurence Brown, Robert Pollard, Sandra Begay, Jana Ganion, and Anya Castillo*.

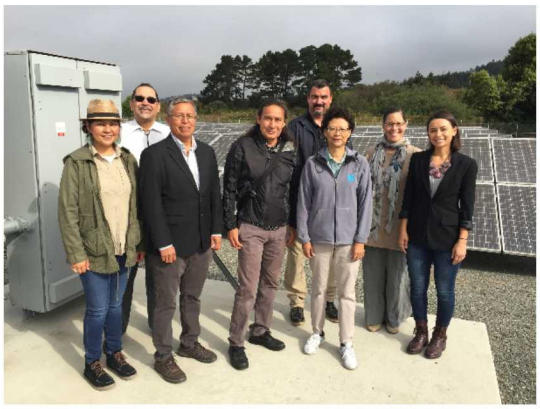


Photo Courtesy of Blue Lake Rancheria Hosts Jana Ganion and Robert Pollard

Figure 2. Sandia Labs Tribal Cyber-Energy Team Visit to Blue Lake Rancheria Microgrid

An example of Energy sector priorities is the Western Regional Partnership (WRP) Strategic Priority for 2019-2020, Source: 2019 WRP Principals' Meeting. The 2019-2020 WRP Strategic Priority is "*Building Resilience in the West for America's Defense, Energy, Environment and Infrastructure through Enhanced Collaboration among Federal, State and Tribal Entities.*"

WRP Committees recommended focus and deep-dives for 2020 in support of the current WRP strategic priority:

- Energy – Resilient Energy Infrastructure
- Military Readiness, Homeland Security, Disaster - Resiliency of Airspace in the WRP Region
- Preparedness and Aviation - Disaster Mitigation
- Natural Resources - Water Security

WRP recommended actions include:

- Identify and outline a Case Study/Pilot Project of an assessment and solution set

[1] Blue Lake Rancheria Micro-Grid Article: https://www.washingtonpost.com/climate-solutions/2020/01/01/amid-shut-off-woes-beacon-energy/?arc404=true

- Contact Sandia Labs to share information on their critical Energy infrastructure security calls (work with stakeholders)
- Western Governors Association's (WGA) collaborative efforts with states to address energy imbalance market
- Department of Defense (DoD): Can they provide a summary of successful efforts to ensure redundant energy supply?
- Microgrids: Feasibility for Tribes, States and other WRP Partners to work with the DoD to enhance energy security. For example, both tribal lands and military bases tend to be in remote areas, and tribal lands frequently possess energy resources. Military bases and tribes could collaboratively create a regional micro-grid, effectively providing distributed deployment of energy and enhancing energy resilience.

1.4. National-Tribal CIP Research and Development

The Tribal-Cyber Energy team has a strong history in supporting critical infrastructure modernization, protection, and resilience. The team has served on past national Tribal Telecom Conference advisory councils, have presented widely at tribal technical conferences and workshops, and at international and national Cybersecurity, Energy, and USG workshops and conferences.

The wide-area interconnectedness and interdependences of the national critical infrastructures demands an increasing scale of integration and collaboration. This need is driven home by two far reaching areas of R&D: Communications and IT Cyber innovation in the changing cyber-ecosystem; and security of discrete critical infrastructure systems that are being modernized by Cyber innovation at an alarming rate.

National-Tribal CIP R&D may be accommodated through many arenas of collaboration. Indeed, each stakeholder area including intergovernmental, industry, and anchor institutions are essential to an inclusive and robust solution. The intergovernmental R&D may include international, national/federal, state, local, tribal, and territorial governments. Of these, other nation states, federal, state, and tribal are recognized as sovereign government entities.

An example of current data analytics R&D is using AI in cybersecurity for strategic energy management. *Dylan Moriarty, who is a citizen of the Navajo Nation and a geoscience engineer is a Sandia Lab's subject matter expert in this R&D area. Dylan was recognized by the American Indian Science and Engineering Society as the Most Promising Engineer/Scientist for 2019. An example of Dylan's work includes Spatiotemporal Data Analytics in Earth, Energy, and Infrastructure as discussed below*:

- The ability to analyze data in both space and time is an essential component of understanding the world we live in. Statistical and machine learning methods are applied to large and sometimes disparate datasets. Some applications include monitoring subsurface locations, analyzing multiphase fluid flow, and critical infrastructure analysis. Multiphase Fluid Property Micro-CT Scan Calculation data analytics is illustrated below:

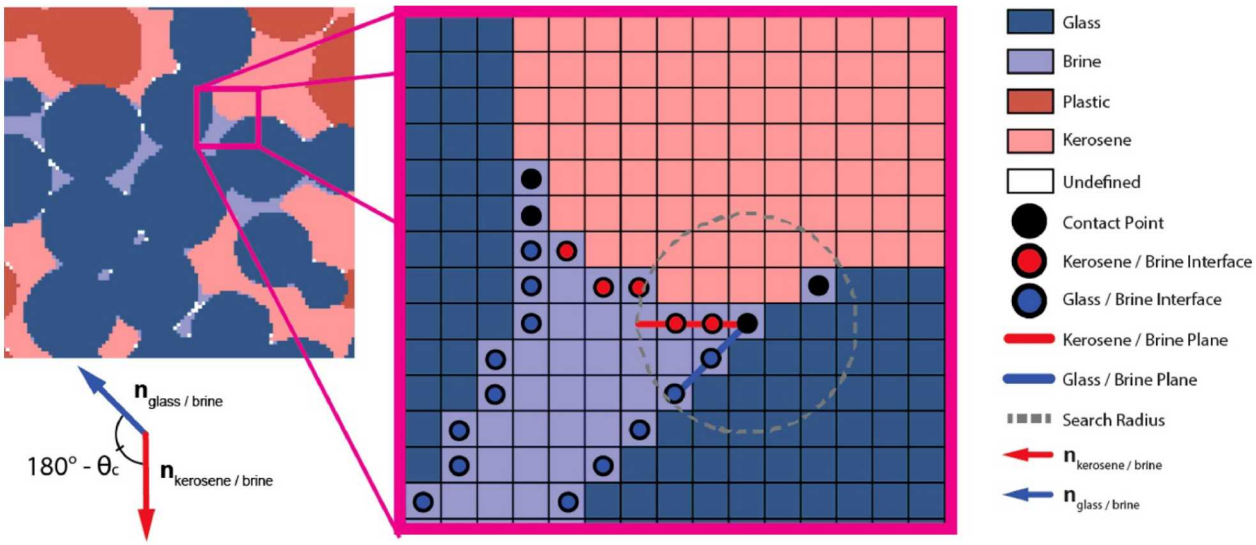


Figure 3. Multiphase Fluid Property (Contact Angle) Micro-CT Scan Calculation

CIP R&D is necessary in virtual, mobile, and internet connected ICS and SCADA systems. Focus could be given to emergent Third Generation Partnership Project (3GPP) 5G New Radio (5G NR or 5G), IPv6 complex integrated systems, and high-performance computing (HPC) data analytics. *Dr. Anya Castillo, Lakota, provides expertise in the area of HPC Cyber-Energy R&D.* These analysis and the following R&D concepts are intended to strengthen preliminary assessment design criteria and for improved preemptive critical infrastructure mitigations.

R&D is needed to develop detection of automated critical infrastructure threats including Bots and BotNets, ransomware, and other automated attacks. Metrics for Mean Time to Detect (MTTD) indicators of compromise (IoC) is an area where understanding the scale of economies for National-Tribal CIP and critical infrastructure interdependencies would elicit extraordinary benefit. Key indicators will need to be defined that can serve as baseline detection metrics from which CIP MTTD may be measured.

Mean Time to Respond ($MTTR^s$) and Recover ($MTTR^c$) is another area where understanding the scale of economies for National-Tribal CIP and critical infrastructure interdependencies is needed. These metrics could map to the NIST Cyber Security Framework (CSF) functions: Detect, Respond and Recover.

Preemptive critical infrastructure mitigation effectiveness can be measured against desired MTTD, $MTTR^s$ and $MTTR^c$ metrics. In this way, CPR design and CSF functions can provide new measures of security assurance.

1.5. Education and Workforce Development

Workforce KSA have been identified as the single most important gap in the changing cyber ecosystem. Infrastructure assessment reveals that older technologies do not scale to today's needs. New standards do scale but are not as well understood or as predominantly deployed. Education and workforce development are keys to enabling scalable and secure National-Tribal CIP. The Nations must have a qualified workforce to engineer, secure, deploy, and maintain next generation national critical infrastructure services into the foreseeable future.

The National Nuclear Security Administration's (NNSA) Minority Serving Institution Partnership Program (MSIPP) is designed to build sustainable pathways between the DOE national laboratories and minority-serving institutions in Science, Technology, Engineering, and Math (STEM) disciplines. The MSIPP program supports ten consortium-based teams. Sandia supports three consortiums; Consortium Enabling Cybersecurity Opportunities and Research (CECOR), Consortium for Integrating Energy Systems in Engineering and Science Education (CIESESE), and the Advanced Manufacturing Network Initiative (AMNI). CECOR's main focus is to establish a world-class workforce development, education and research program that combines the strengths of Historically Black Colleges and Universities (HBCUs) and Sandia Labs to develop a K-20 pathway for students to participate in cybersecurity and other STEM fields. CIESESE provides opportunities for students from Hispanic Serving Institutions (HSI) to pursue studies and careers in energy systems R&D. AMNI's goal is to establish a network of Tribal Colleges and Universities (TCUs) with essential advanced manufacturing facilities, associated training and education programs,

and private and federal agency partnerships to both prepare an American Indian workforce and create economic and employment opportunities within tribal communities through design and manufacture of high quality parts.

Source: Sandia National Laboratories CECOR Program

Figure 4. Consortium Enabling Cybersecurity Opportunities & Research

Figure 5. Consortium for Integrating Energy Systems in Engineering & Science Education

Figure 6. Advanced Manufacturing Initiative Network led by the American Indian Higher Education Consortium

Regarding the AMNI consortium, Sandia Labs is providing technical advising, planning and academic program development support to TCUs and is working closely with the American Indian Higher Education Consortium (AIHEC), which oversees the AMNI consortium. There are currently 75 TCU campuses in 16 states which are chartered by their respective tribal governments. AIHEC, which represents the interest of TCUs, helps ensure that the principal of tribal sovereignty is recognized and respected. AMNI consortium includes TCUs from Navajo Technical University (NTU), Salish Kootenai College (SKC), Cankdeska Cikana Community College (CCCC), Turtle Mountain Community College (TMCC), and Bay Mills Community College (BMCC). These TCU's have established strong pre-engineering and engineering programs. The NTU: http://www.navajotech.edu/ is an example of tribal STEM educational successes in Sandia Labs regional area. Through Sandia's Engineering Advisory Board leadership at NTU, NTU received accreditation through the Accreditation Board for Engineering and Technology (ABET) for their Electrical and Industrial Engineering programs. This is a significant milestone that will

significantly expand the students' opportunities and marketability as they enter the workplace. Sandia Labs has hired several American Indian summer intern students through this program since 2016. Educational programs such as these are a resounding success due to exceptional educational leaders, although more is needed.

The award winning Southwest Indian Polytechnic Institute (SIPI): https://www.sipi.edu/, is another example of tribal STEM educational successes in Sandia Labs regional area. In light of the extraordinary benefits envisioned herein, strengthened TCU MSIPP support, such as cyber-physical-resilient design practices, would elicit immediate value for tribes getting broadband capability for the first time.

Next generation cyber and energy workforce is a national priority and immediate need. Sandia Labs is an exceptional STEM facilitator. The Tribal-Cyber Energy team has a strong history in supporting STEM. In addition to the aforementioned successes, the team has provided support to a 2018 Mississippi Band of Choctaw Indians Hackathon for high school and college students. This is an example of how national priority need can be met by tapping the intellectual capacity and passion of underrepresented students and populations. Thus, delivering extraordinary National-Tribal CIP workforce benefit.

1.6. Critical Infrastructure Digital Transformation

A disciplined "baked-in" security approach is needed and can be facilitated by National-Tribal CIP. Critical infrastructure digital transformation creates a new paradigm of connectivity and computational capabilities, which include vast sensor networks and IoT instrumentation.

The impact of the digital dichotomy represents changes in standards for IT and Communications IP, mobile RF communications, and virtual technologies. One may consider the IoT, Mobile IoT, and Industrial IoT as a means of instrumentation for smart-grid, smart-agriculture, and automated self-driving vehicles. These IoT instantiations and changes in standards are significant in digital transformation across the sixteen DHS defined critical infrastructure sectors.

Lastly, consider the impact of virtualization, including Cloud, Artificial Intelligence (AI), Machine Learning (ML), VR, and AR in modernized ICS and SCADA systems. These computationally advanced software systems add to the notion of data everywhere. A paradigm of Data Everywhere-User Anywhere becomes apparent when Cloud is coupled with mobility. These advances effectively evaporate the classic enterprise network perimeter. A new approach to data-centric information protection is needed. National-Tribal CIP can lead to more secure innovation at scale in new internet services in expanded broadband service areas for modernized ICS and SCADA systems.

1.7. Risks, Attack Surface, and Mitigations

It is often said that Cybersecurity is asymmetric: an attacker must find one way in to be successful, a defender must protect everything. This section addresses high-level risks, attack surface, and National-Tribal CIP mitigations.

Outdated cyber-infrastructure risk is built on a bolt-on security model, where products are released with security as a secondary concern, if at all. Bolt-on security results a continual pursuit to secure cyber-infrastructure after the fact of product release. Modernized cyber-infrastructure risk involves emergent risk, where newer technologies are not as widely deployed and understood. Modernization also comprises large-scale integration of IT/OT/IoT, and virtualized automation. The key mitigation is a knowledgeable workforce. These trends are particularly evident across the sixteen DHS defined critical infrastructure sectors. The digital dichotomy of old and new technologies exacerbates risk in a larger and sometimes uncontrolled attack surface. Two key mitigations include divestiture of legacy technologies to reduce the attack surface, and investing in scalable standards-based technologies.

The broad risk perspective includes National-Tribal collective critical infrastructure risk. National risk includes federal, private sector, and SLTT critical infrastructure stakeholders. Converging IT/OT/IoT infrastructures are in large part representative of expanding critical infrastructure attack surfaces. The key mitigations are to design-in security and collaborate at the National-Tribal CIP scale.

The table below illustrates concerns at a high-level of risk, attack surface, and mitigation.

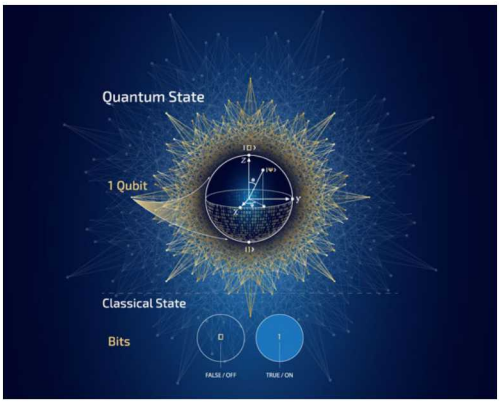
Table 2. High-Level Risks, Attack Surface, and Mitigation

Risk	Attack Surface	Mitigation
Outdated Cyber Infrastructure Risk	Well Known Threat, Vulnerabilities, and Exposure	Continual Cybersecurity pursuits in insufficient Bolt-On after release security
Modernized Cyber Infrastructure Risk	Emerging Threat, Vulnerabilities, and Exposure	Stakeholder and Workforce Education and KSA Development
Digital Dichotomy Complexity Risk	Combined Threat, Vulnerabilities, and Exposure	Invest in Scalable Standards Based Technologies, Divest Legacy Technologies
National-Tribal Critical Infrastructure Risk	Multi-Stakeholder Converging IT/OT/IoT Threat, Vulnerability, and Exposure	Secure Design Build, CPR Design, Collaborate at the National-Tribal CIP Scale

Much more technical detail is included in the Cyber Modernization section of this report, which is intended to shed light on subsequent complexities as a current state deep-dive. The composite technological and national security impacts are of great common concern.

1.8. Sandia Labs World-Class Science and Engineering

Sandia Labs Center for Computing Research is a world-class high-performance computing capability. For example, Sandia Labs provides leadership for the Quantum Information Edge, a nationwide alliance of national laboratories and universities, launched to maintain U.S. leadership in next-generation information technology and advance the frontiers of quantum computing systems, which have the potential to make calculations that are far beyond the reach of today's computers. This is representative of a future forward vision, where for example, Quantum State Cybersecurity could be applied for extraordinary shared CIP benefits.



Source: Sandia National laboratories, Credit Michael Vittatow

Figure 7. Quantum State Illustration

Another example of Sandia Labs leadership in innovation is the Idea Lab that fosters collaborative Augmented Reality (AR) Virtual Reality (VR). The CARVR Idea Lab has been designed to allow anyone that can connect to the Sandia Network from any device, to collaborate. Different collaborators can be in a virtual environment, with a VR headset or on a computer using their keyboard to navigate. As a visualization lab, it's important to allow people to share their ideas in a variety of ways. The image shows an example of how a computer model can be viewed in VR and in AR with enough realism to make the computer model seem real.

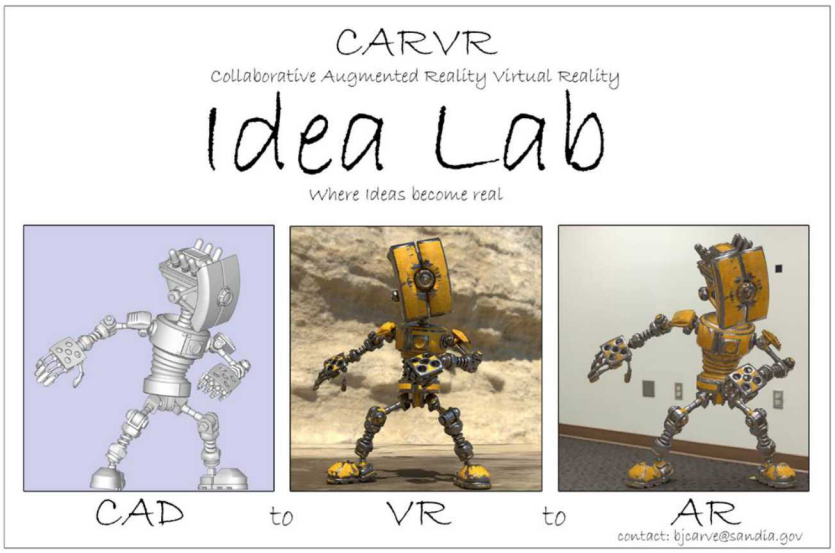


Figure 8. CARVR Idea Lab

Another notable data science success is Slycat™, which is a web-based system for performing data analysis and visualization of potentially large quantities of remote, high-dimensional data. Slycat™ specializes in working with ensemble data. An ensemble is a group of related data sets, which typically consists of a set of simulation runs exploring the same problem space. An ensemble can be thought of as a set of samples within a multi-variate domain, where each sample is a vector whose value defines a point in high-dimensional space. To understand and describe the underlying problem being modeled in the simulations, ensemble analysis looks for shared behaviors and common features across the group of runs. Additionally, ensemble analysis tries to quantify differences found in any members that deviate from the rest of the group. The Slycat™ system integrates data management, scalable analysis, and visualization. Examples of Slycat™ data science innovation are illustrated below, Each model is showing a different results type (table on the top, time series on the bottom) from the same 15K run ensemble.

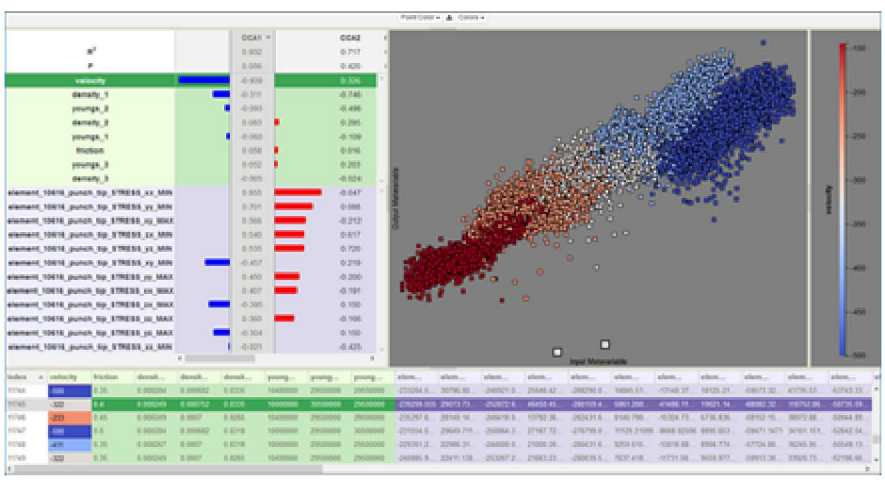
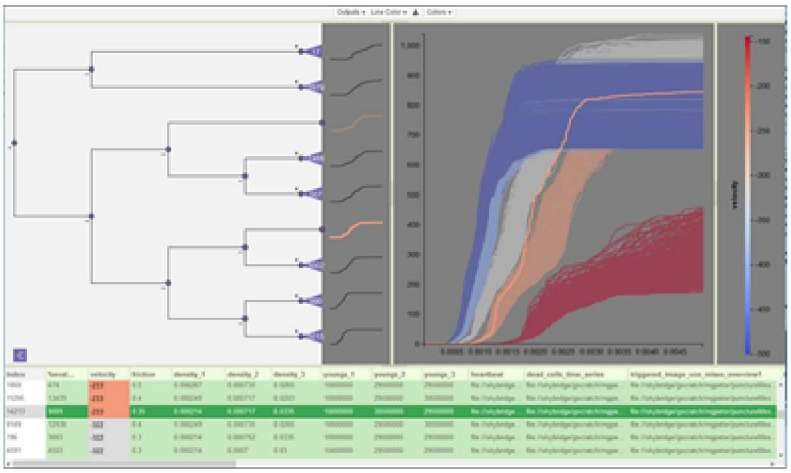


Figure 9. SlyCat Table View



Source: Sandia National Laboratories Center for Computing Research

Figure 10. SlyCat Time Series View

These world-class science and engineering capabilities position Sandia Labs as strong facilitating partner, provided that eventual federal funds availability could support a National-Tribal CIP mission vision. Further information is available at Sandia Labs website: www.sandia.gov.

1.9. Project Costs and Estimates

Sandia Labs has a successful record of tribal technical assistance projects. The team relies on several project vehicles to collaborate with AI/AN Tribal Government stakeholders. The focus has been local small business technical assistance and regional tribal wide-area technical assistance. Work has been conducted with individual tribes and tribal consortia, although the goal has always been a national-tribal level of effort.

NMSBA projects allow us to provide technical assistance to tribally affiliated small business in New Mexico. Project successes include telecoms providing expanded broadband services, emergency management needing broadband access in association with the MRGTPC.

SPP have been funded through Tribal application and award from the Tribal Homeland Security Grants Program (THSGP). Results include successful project completion for national, multi-state, and tribal stakeholder's emergency services modernization and resilience.

Table 3. National-Tribal CIP Estimated Scale, Cost, and Value

Project Scale	Cost	Value
Past NMSBA Projects	$40K each	Technical Assistance To NM Small Businesses, estimated at $10k-$100k economic development
Past SPP Projects	$500K each	Regional Technical Security and Resilience, potentially $1M in recovery and hidden cost avoidance
Proposed Individual National-Tribal CIP Projects	$500K to $1M each	Tribal Stakeholder Technical Advantage made available to National Stakeholders, potentially $10M in recovery and hidden cost avoidance
Proposed National-Tribal Consortium CIP Projects	$1M to $10M each	Regional Tribal Stakeholder Technical Advantage made available to National Stakeholders, potentially $100M in recovery and hidden cost avoidance

The Tribal Cyber initiative has been successful on a project by project basis with relationship and statement of work development facilitated by Sandia Labs Tribal Government Relations Executive Office program development funds. Project successes are due to those funds as well as staff expertise and participation at the national security priority

scale that informs Tribal Cyber-Energy work. The convergence of Tribal Cyber-Energy work has been an obvious progression with regard to emergent smart-grid requirements for communications, IT, OT and the various instantiations of the IoT.

The Tribal Cyber initiative has not been funded at a programmatic level. Federal sponsorship at a programmatic level is a goal for National-Tribal CIP collaboration. Tribal Energy work has a more substantial programmatic funding posture. Tribal Cyber-Energy work expands on energy focus and offers nearly unbounded R&D opportunities that would require a programmatic funding posture for viability and sustainability. Concerns at the programmatic level of activity are staffing and authority to conduct work at the National-Tribal scale.

1.10. Critical Infrastructure Protection - Extraordinary Benefits

Objective Science and Engineering: The Sandia Labs Tribal Cyber-Energy team is uniquely composed of subject matter experts who understand world class science and engineering and are also American Indian tribal citizens and/or of Native Hawaiian ethnicity. Thus, the team has a unique understanding of the extraordinary benefits possible through objective advisory and collaborative National-Tribal CIP.

Single Point of Authority: American Indian Sovereign Governments have single point of authority over their critical infrastructures. National-Tribal CIP collaboration presents a path to extraordinary benefits as tribal areas gain access to broadband services with the opportunity to build better and more secure with scalable technologies. A path forward for educated tribal people to work from their communities would greatly enhance tribal capabilities. AI/AN creators of Internet content makes the Internet better for everyone.

National Critical Infrastructures: The national critical infrastructure fabric is woven by and inclusive of all critical infrastructure stakeholders. Partnership with national stakeholders offers extraordinary benefits at the national scale: where national critical infrastructure priorities may be solved faster, better, and more secure with scalable solutions developed at tribal scales then applied at the national scale.

Extraordinary Benefits: The vision of extraordinary benefits is inclusive of all critical infrastructure stakeholders. The combined scientific advancement, modernized, secure and resilient national security capabilities have proven value demonstrated through significant accomplishments. For example, National-Tribal CIP extraordinary benefits could address DHS Cybersecurity and Infrastructure Security Agency (CISA) SLTT CIP priorities: https://www.cisa.gov/. Results could also inform and enhance the CISA National Cybersecurity Protection System (NCPS): https://www.cisa.gov/national-cybersecurity-protection-system-ncps. Taken together, extraordinary national security advantage can be gained through collaborative National-Tribal CIP.

2. THE POWER OF COLLABORATION

Tribes are underrepresented in national broadband access at the same time as access is expanding and tribes recognize the need for advanced Internet services. Security and resilience are overriding concerns. National-Tribal collaboration offers secure and resilient expanded access with mutually beneficial advancement. Collaboration is a partnership with the human factor at the core of design, use, security and risk management. Systems, networks and critical infrastructures are built by us, for us, and to the benefit of our communities. Collaboration is the key to successful modernization, use, and security of critical infrastructure lifecycles in times of normal operations and resilience during disruptive events.

Sandia Labs has been at the forefront of national security as a world class science and engineering laboratory since its inception. National security is a collective multi-stakeholder concern that is daunting at every level, in particular at this time of disruptive critical infrastructure modernization.

The Sandia Labs Tribal Cyber-Energy initiative began from two separate mission concerns: Cyber and Energy. The Energy and Cyber areas of concern ultimately converged as it became apparent that the Energy divide and the Digital divide are congruent: Energy infrastructure enables IT and Communications infrastructure, and in turn, IT and Communications infrastructure enables Energy infrastructure, as is the case with Smart-Grid, Smart-Metering, and microgrid modernization. In short, cyber needs energy and energy needs cyber.

Similar Cyber advancements are at hand across all critical infrastructure sectors nation-wide, and AI/AN nations wide. In terms of critical infrastructure, modernization renders an increased attack surface. Again, the power of collaboration is the key to shared and secure critical infrastructure solutions.

2.1. U. S. Government and Tribal Collaboration

U.S. Government (USG) and Tribal engagement addresses the need for improved CIP as critical infrastructures span geography and federal and tribal critical infrastructure stakeholder interests. Negotiated accesses through treaties and a distinguished set of self-governance rights follows a trust responsibility of the USG for tribes. American Indian tribes are both ethnic and cultural, and sovereign government entities. According to a recent First Nations Development Institute report (www.firstnations.org): Tribes are second only to the U.S. government in land holdings. Figure 2 below illustrates Native American and Alaska Native lands, circa 2010 Census Bureau results.

Source: https://www2.census.gov › special › AIANWall2010 › AIAN_US_2010

Figure 11. Native Americans and Alaska Natives in the United States

Broadband expansion is a worldwide event and a national priority. The vast expansion of connectivity precedes the availability of advanced Internet Services in rural America and in Indian Country: The Energy and Digital divides are closing, but there is an accompanying digital dichotomy where older technologies are being supplanted by newer more scalable technologies.

The changing cyber ecosystem emphasizes the need for Intergovernmental and AI/AN Tribal Government stakeholder collaboration, which is intended to serve a broad set of critical infrastructure interests across Agencies and all federally recognized tribes.

2.1.1. Department of Interior

Department of Interior (DOI) collaboration implies strong intergovernmental and tribal stakeholder coordination. Such collaborative engagement is necessary to meet the common goals of many stakeholders. This review begins with the DOI hierarchy as illustrated below.

Department of Interior Organizational Chart

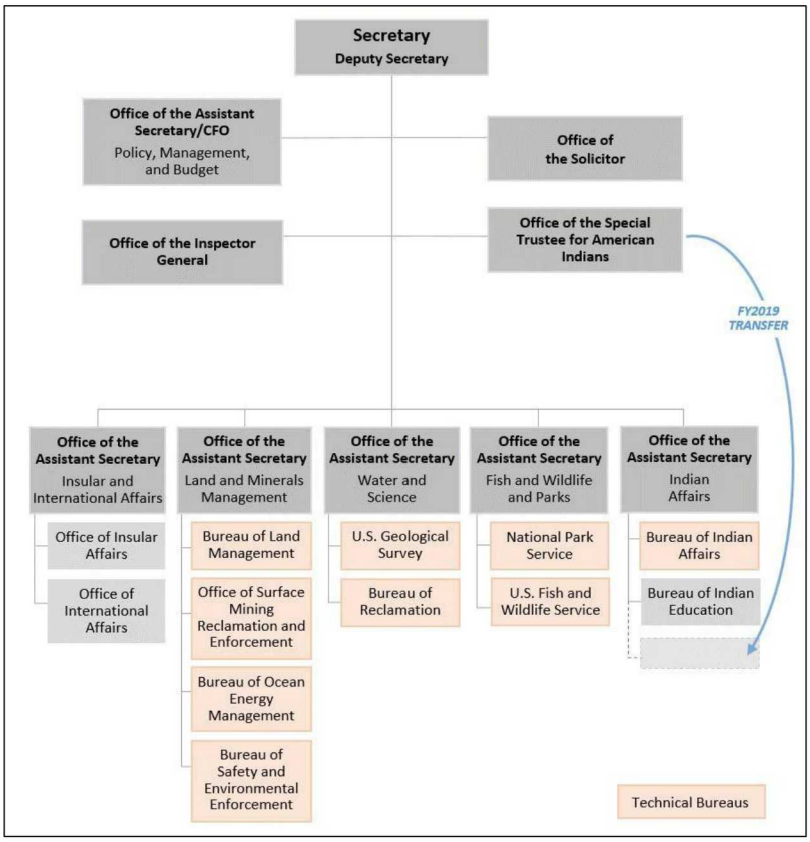


Figure 11. Department of Interior Hierarchy Structure

Figure 7[2] illustrates alignment within the Bureau of Indian Affairs (BIA). The BIA falls under the DOI at the federal level of government in the Executive Branch. Understanding the role of federal government stewardship is a very important aspect in tribal infrastructure modernization strategic planning initiatives.

Established in 1824, the BIA is the oldest bureau within DOI, predating the department by 25 years. Then Secretary of War John C. Calhoun established the Office of Indian Affairs to help centralize what was at the time a fractured administrative approach to Indian policy and relations in the United States.[25] It was not until 1832 that Congress officially recognized the Office of Indian Affairs as a bureau of the War Department by appointing a commissioner

[2] https://www.doi.gov/sites/doi.gov/files/uploads/fy2019_os_budget_justification.pdf

to oversee the agency. The Office of Indian Affairs was transferred to DOI in 1849, when the department was created. DOI formally adopted the name *Bureau of Indian Affairs* in 1947.

The BIA is broken into twelve (12) different regional geographical areas and there is a headquarters in each of the regional areas. The regional headquarters for the Southwest Region is located in Albuquerque, New Mexico. The regional offices share in the responsibility in understanding government rules and regulations, strategic planning and acquiring grant money for advancements in areas for broadband network modernization initiatives.

Bureau of Indian Affairs (BIA)

Established: 1824

Key Statute: Snyder Act of 1921 (42 Stat. 208)

Mission: "To enhance the quality of life, to promote economic opportunity, and to carry out the responsibility to protect and improve the trust assets of American Indians, Indian Tribes, and Alaska Natives."

Leadership: Director

Headquarters: Washington, DC

Average Staff: 7,600 (including staff from the Bureau of Indian Education)

Regions: 12

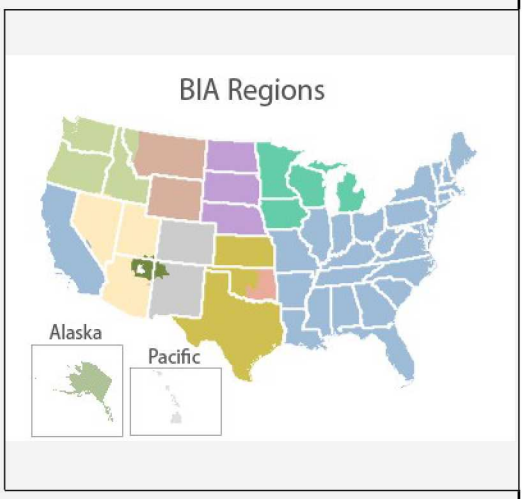


Figure 12. Bureau of Indian Affairs, "About Us"

BIA[3], provides services to federally recognized AI/AN tribes and their nearly 1.9 million members. These services include disaster relief, child welfare, and road construction, as well as the operation and funding of law enforcement, tribal courts, and detention facilities within native villages and reservations. The bureau also is responsible for protecting and administering assets on tribal lands, including the management of 55 million surface acres and 57 million acres of subsurface mineral estates held in trust by the United States.

The BIA was also previously responsible for providing elementary and secondary education and educational assistance to Indian children through BIA's Office of Indian Education Programs. In 2006, however, the Secretary of the Interior separated the BIA education programs from the rest of the BIA and placed them in a new Bureau of Indian Education (BIE) under the Assistant Secretary–Indian Affairs. As of FY2018, the BIE education system served approximately 47,000 students through 169 elementary/secondary schools and 14 dormitories located in 23 states. For the purposes of this report, BIE is not considered a *technical bureau* of DOI. However, BIE employment figures are included in BIA totals.

The BIA is administered by a director who oversees the agency's functions and reports to the Assistant Secretary of Indian Affairs. Similar to other DOI agencies, the BIA has a three-tiered organizational structure, with leadership and senior executives operating from headquarters in Washington, DC, and 12 regional offices that oversee 53 field offices (referred to as *agencies* by the BIA); these agencies deliver program services directly to tribal communities. As of June 2018, the BIA and BIE combined had roughly 7,000 employees.

Without working through the BIA, for the advancement of broadband wireless and land mobile radio telecommunications and cyber security, every sovereign nation will be working on individual projects instead of working on a nations-wide strategy. The ability to bridge the digital divide may be completed by individual projects within every sovereign nation but ideas, successes and failures in the deployment of technologies and grant money should be communicated through various methods.

[3] https://www.bia.gov/about-us.

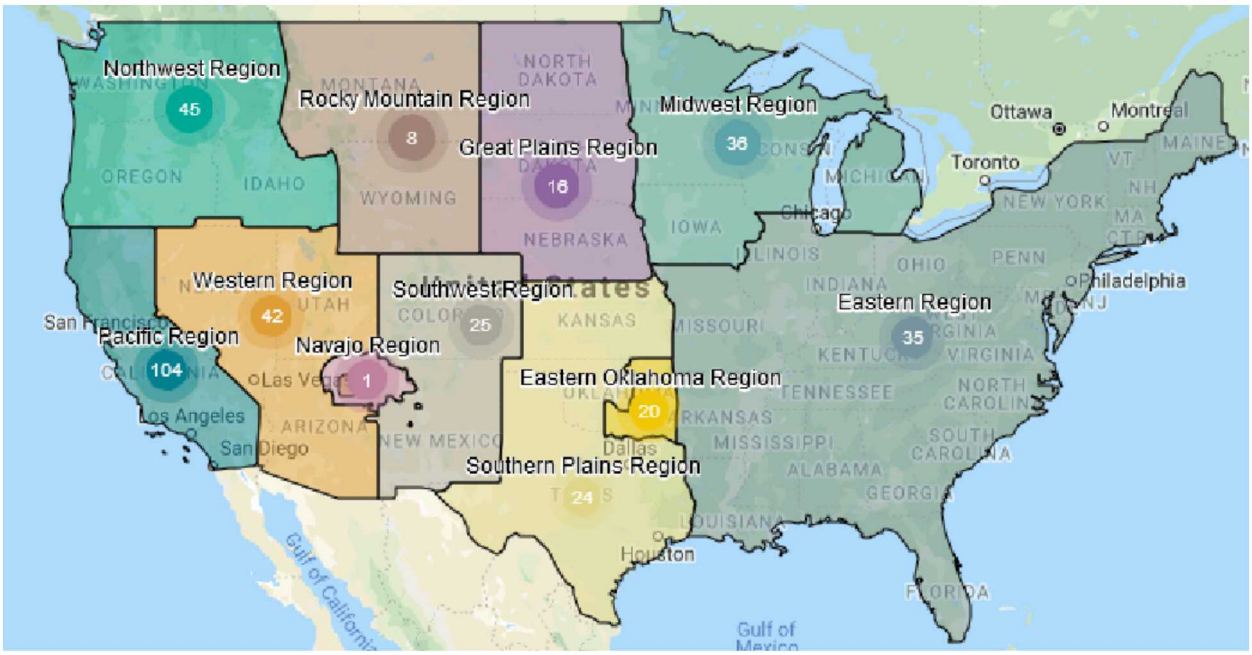


Figure 13. BIA Regional areas in continental United States excluding Alaska/Hawaii

2.1.2. DOI Office of Chief Information Officer – Telecommunications

Telecommunications provide the DOI and other supported federal agencies, tribal nations, and insular areas with IT and connectivity and/or services for the delivery of video, voice and data to meet the Department's mission.

Telecommunications support extends to over 3000 sites throughout all 50 states and at other locations from the US Virgin Islands westward to Palau, and from Alaska to American Samoa in the Southern Hemisphere. DOI's locations include some of the most remote and challenging locations to ensure connectivity, with the added complexity of not detracting from pristine natural resources and surroundings. IT and communication services consists of three primary operational functions - each of which serves as a key link in supporting mission requirements across the Department. The three functions are: Voice Services, Network Services, and Radio Communications and Spectrum services.

2.1.2.1. Voice Services

Voice services throughout the Department are handled by a number of offices, depending on the specific needs of the locations and/or the mission requirements. Voice services performed within the Office of the Chief Information Officer include:

- Managing the voice network that supports all DOI bureaus and offices within the headquarters building in Washington DC
- Managing voice support for critical locations in Virginia, Colorado, and Arizona
- Supporting and/or managing audio bridge conferencing, video teleconferencing, 1-800 numbers, cellular phones, billing, etc.

2.1.2.2. Network Services

Network Services provides the backbone architecture that connects to the Internet in order to exchange information across the Department. Network services performed within the Office of the Chief Information Officer include:

- Managing network gateways/Trusted Internet Connections in five states supporting the needs of over 300,000 DOI employees and volunteers.

- Coordinating support for the "last mile" connectivity to more than 2000 National Parks, Wildlife Refuges, National Monuments, fish hatcheries, other units and scientific sensors located in all 50 states.
- Providing WiFi connectivity and management at several DOI locations.
- Overseeing overall IT availability, status, mitigation, and restoration efforts during natural disasters and other national crises
- Supporting over 50 federal agencies and 300,000 employees across the US government with secure IT to deliver over $25 billion in annual payroll, to conduct official government travel, to give human resource assistance, and to provide other essential services.

2.1.2.3. Radio Communications & Spectrum Services

Radio Communications & Spectrum services[4] at DOI are essential for successful field operations that range from law enforcement activities to wildfire response coordination with other federal, state, tribal, and local authorities to first responder support during national emergencies. Services performed within the Office of the Chief Information Officer include:

- Manage technical services, enterprise contracts, and develop radio standards and architecture
- Operate the National Radio Laboratory for testing performance, interoperability, software update validations
- Support for radio systems used by the Secretary and other ranking officials in the Department
- Manage, allocation and interference deconfliction of all radio frequencies used by DOI customers, insular areas, and supported external customers. This includes incident/emergency support for wildland fires, hurricanes, floods, etc.
- Coordination of spectrum and radio sharing with federal, state, local, and international agencies.

Relying on cellular devices is a trend that continues. It is important to have a backup method of communicating with the workforce, first responders, and emergency management personnel. One method that works effectively is through the use of a licensed P-25 land mobile radio architecture. Leased radios from a valid FCC license holder is another way to ensure that land mobile radio communications exist. An effective telecommunications architecture is illustrated below.

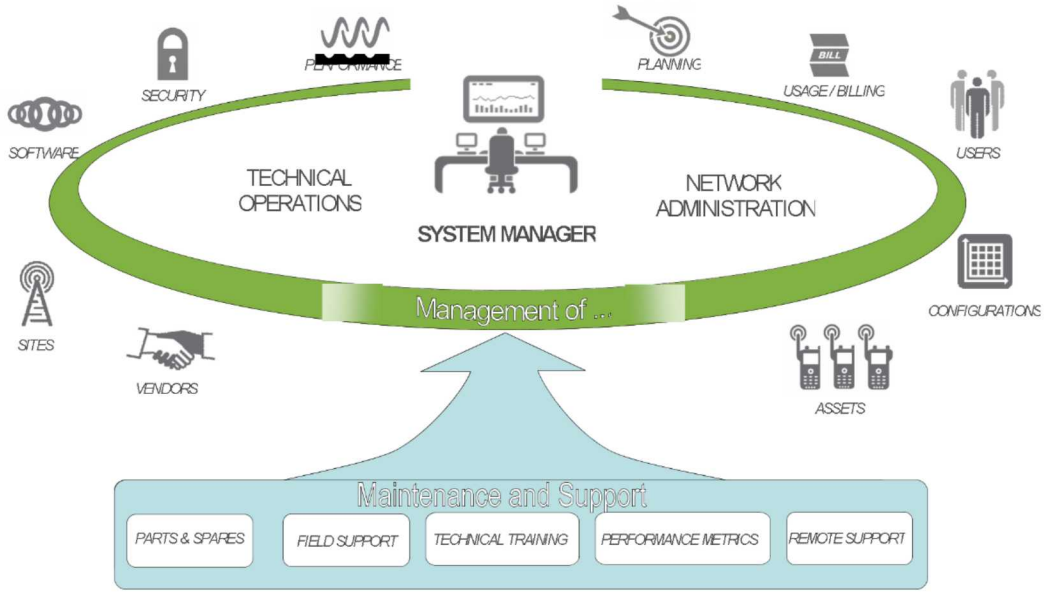


Figure 14. Chart for Effective Telecommunications Architecture

[4] Source: https://www.doi.gov/ocio/customers/telecommunications

Long haul RF microwaves is an effective method to utilize when there is no existing fiber or copper. Because the American Indian community falls under the BIA, it is possible to submit and acquire licensed radio frequency authorizations through the BIA to the DOI spectrum management community. The DOI Frequency Assignment Subcommittee person would have to submit requests through the NTIA. Paired frequencies that are licensed would ensure no negative RF interference as compared to using unlicensed RF microwave equipment. There are many vendors that manufacture and sell licensed RF microwaves for this purpose.

Point to multipoint RF Microwave architectures are being used effectively in many rural areas. The benefit of these architectures is to put up a single command and control microwave and several base station units to various locations that require higher speed data rates. These systems are unlicensed FCC certified microwave architectures.

The DOI utilizes the Government Master File (GMF) along with other federal government departments. There is also the Spectrum XXI database which is heavily used by the Department of Defense and other federal government departments. Managing the utilization of spectrum dependent services is complex and without a database to catalogue all licensed and unlicensed radio frequency authorizations, will eventually lead to a cluttered radio frequency environment with the potential for harmful radio frequency interference among users.

2.1.3. Interdepartment Radio Advisory Committee (IRAC):

The basic functions of the IRAC are to assist the Assistant Secretary in assigning frequencies to U.S. Government radio stations and in developing and executing policies, programs, procedures, and technical criteria pertaining to the allocation, management, and use of the electromagnetic spectrum. The basic role of the representatives appointed to serve on the IRAC is to function, when in Committee, in the interest of the United States as a whole.

Composition of the IRAC:

- Members: Dept. of Agriculture, Air Force, Army, Coast Guard, Dept. of Commerce, Dept. of Energy, Federal Aviation Administration, Dept. of Homeland Security, Dept. of the Interior, Dept. of Justice, National Aeronautics and Space Administration, Navy, National Science Foundation, Dept. of State, Dept. of Transportation, Dept. of the Treasury, United States Agency for Global Media, United States Postal Service, Dept. of Veterans Affairs
- Liaison: Federal Communications Commission

Substructure of the IRAC

The permanent substructure of the IRAC consists of the IRAC Secretariat and the:

- Emergency Planning Subcommittee (EPS)
- Frequency Assignment Subcommittee (FAS)
- Radio Conference Subcommittee (RCS)
- Space Systems Subcommittee (SSS)
- Spectrum Planning Subcommittee (SPS)
- Technical Subcommittee (TSC)

The IRAC may create subcommittees, ad hoc, or working groups to deal with specific topics

Source: https://www.ntia.doc.gov/page/interdepartment-radio-advisory-committee-irac

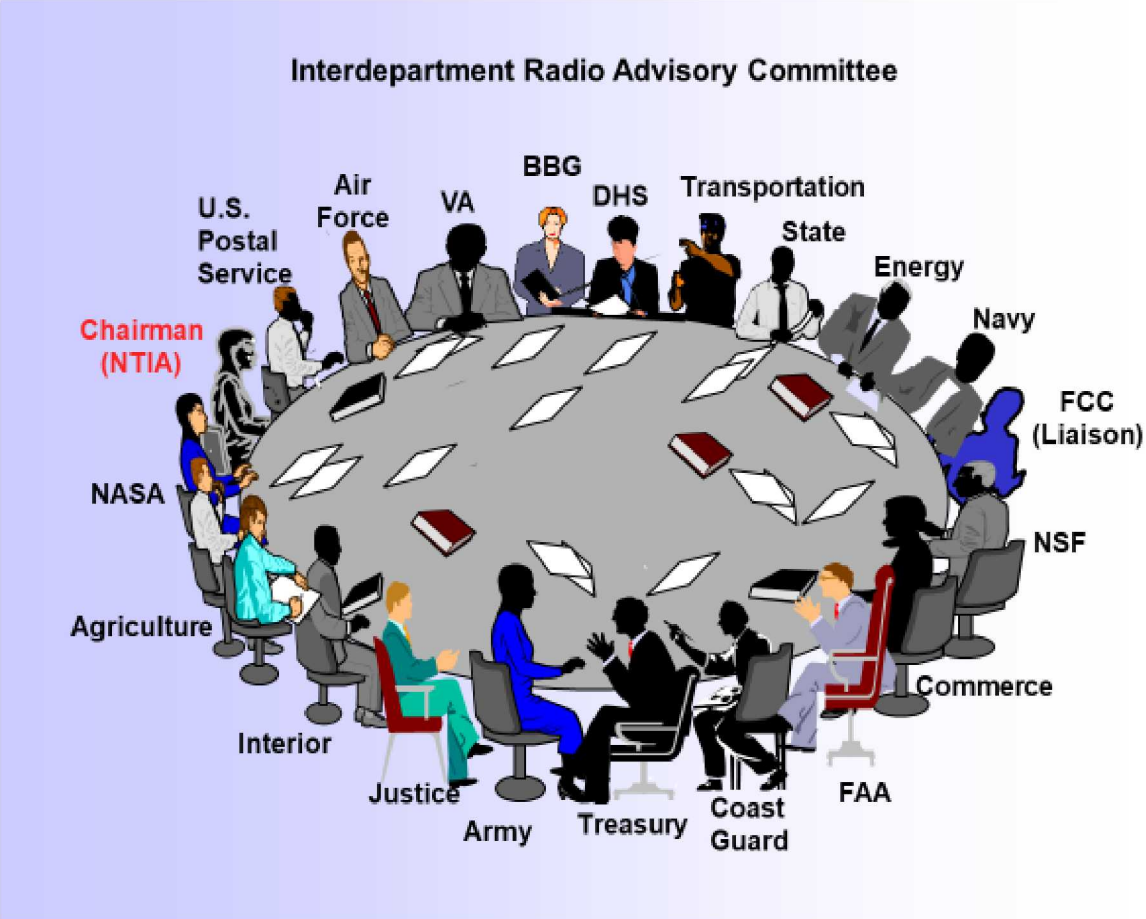


Figure 15. IRAC Members

IRAC members are able to liaison with the FCC. An important consideration is the possibility of creating a National-Tribal subcommittee to address broadband networking in rural AI/AN lands. Without a National-Tribal subcommittee, much information will continue to be lost and not captured for the advancement of rural broadband initiatives. Such a subcommittee with tribal representation could address complex challenges such as modernization and right of way easement concerns, which are very complex, particularly in tribal checkerboard areas.

2.1.4. FCC Initiatives and Findings

The Federal Communications Commission (FCC), an independent U.S. government agency overseen by congress is also very important in tribal infrastructure modernization strategic planning initiatives. For example, spectrum sovereignty concerns and wireless access for tribal communities. The FCC has recently created reports dealing with broadband internet and tribal broadband, Excerpts from recent findings is provided below. A national database of federally licensed radio frequency authorizations exists today.

2.1.4.1. Recommendations for Executive Action

- Broadband Internet: FCC's Data Overstate Access on Tribal Lands, GAO-18-630: Published: Sep 7, 2018. Publicly Released: Sep 7, 2018

  Status: Open

  Recommendation: The Chairman of the Federal Communications Commission should develop a formal process to obtain tribal input on the accuracy of provider-submitted broadband data that includes outreach and technical assistance to help tribes participate in the process.

  Agency Affected: Federal Communications Commission

- August 6, 2019, FCC report and order of proposed rulemaking focused on improving FCC's broadband data

Status: Open

Comments: On August 6, 2019, the FCC issued a report and order and a further notice of proposed rulemaking focused on improving FCC's broadband data. The report and order directed an FCC contractor, in coordination with FCC offices and bureaus, to establish the Digital Opportunity Data Collection, which requires fixed broadband providers to submit more granular geographic data (polygons) depicting their service areas. The filings must reflect the maximum download and upload speeds actually made available in each area. FCC also noted that for the purposes of this data collection, service is actually available in an area if the reporting fixed provider has a current broadband connection or it could provide such a connection within ten business days of a customer request, without an extraordinary commitment of resources, and without construction charges or fees exceeding an ordinary service activation fee. The broadband provider must also be able to establish a connection within this timeframe to every end-user location contained in the reported broadband coverage polygon. FCC also directed its contractor to develop a mechanism to verify the data and to collect input from tribal governments and the public on the data. FCC sought comment on establishing technical parameters when considering whether service could be made available in an area, and stated that it would consider the results of this effort and determine whether to apply it to mobile broadband providers as well. FCC also sought comment on how its contractor could assess coverage disputes, and how it should best incorporate input from tribal governments on broadband coverage maps. We will continue to monitor FCC's implementation of these efforts.

Recommendation: The Chairman of the Federal Communications Commission should develop and implement methods, such as a targeted data collection, for collecting and reporting accurate and complete data on broadband access specific to tribal lands.

Agency Affected: Federal Communications Commission

FCC Concurrence with this Recommendation

Status: Open

Comments: FCC concurred with this recommendation and said it would take steps to implement it. When we confirm what actions FCC has taken in response to this recommendation, we will provide updated information.

- October 24, 2018, FCC Appointment of Members to the FCC's Native Nations Communications Task Force

  Status: Open

  Comments: On October 24, 2018, FCC announced the appointment of 19 Tribal members and eight FCC members to the FCC's renewed Native Nations Communications Task Force. The Task Force, according to FCC's website, "will help the Commission fulfill its commitment to increase access to broadband and other communications infrastructure deployment and services on Tribal lands." According to FCC officials, FCC has tasked the Native Nations Communications Task Force with helping evaluate the effectiveness of the tribal engagement obligation, and expects the task force to provide FCC with its findings and recommendations by Spring 2020. We will continue to monitor FCC's implementation of these efforts.

  Recommendation: The Chairman of the Federal Communications Commission should obtain feedback from tribal stakeholders and providers on the effectiveness of FCC's 2012 statement to providers on how to fulfill their tribal engagement requirements to determine whether FCC needs to clarify the agency's tribal engagement statement.

  Agency Affected: Federal Communications Commission

- Tribal Broadband: FCC Should Undertake Efforts to Better Promote Tribal Access to Spectrum, GAO-19-75: Published: Nov 14, 2018. Publicly Released: Nov 14, 2018.
- July 2019, FCC Collection of Data on Tribal Entities Obtaining and Accessing spectrum.

  Status: Open

  Comments: As of July 2019, FCC said it will consider ways to collect data on the extent that tribal entities are obtaining and accessing spectrum, including updating application forms to provide for voluntary submission of this information. FCC noted that this is an ongoing activity with no specific completion date.

  Recommendation: The Chairman of FCC should collect data on the extent that tribal entities are obtaining and accessing spectrum and use this information as FCC implements ongoing spectrum initiatives.

Agency Affected: Federal Communications Commission

- July 2019, FCC Plans to Sample Spectrum Licenses on Tribal Lands

  Status: Open

  Comments: As of July 2019, FCC indicated it plans to take a sample of spectrum licenses on tribal lands and then analyze these data to inform its spectrum policies. FCC expects the analysis to be completed by the end of 2019.

  Recommendation: The Chairman of FCC should analyze data to better understand the extent that unused spectrum licenses exist over tribal lands, such as by analyzing the data for a sample of tribal lands, and as appropriate use this information to inform its oversight of the secondary market.

  Agency Affected: Federal Communications Commission

- July 2019, FCC Engagement in a Multi-Year Project to Modernize the Universal Licensing System

  Status: Open

  Comments: As of July 2019, FCC said it was engaged in a multi-year project to modernize the Universal Licensing System (ULS), which is the online system that contains electronic records of all wireless spectrum licenses. FCC said it would transition ULS to a new platform that will provide more consistent performance, easier access to information, and enhanced functionality; the ULS modernization is an ongoing activity with no specific completion date. Additionally, FCC noted that it's Office of Native Affairs and Policy provides tribes with information about accessing ULS and opportunities to access spectrum through new licenses, as well as through partitioning, disaggregating, and leasing existing spectrum licenses.

  Recommendation: The Chairman of FCC should make information on spectrum-license holders more accessible, and easy to understand for interested parties, including tribal entities, to promote their ability to purchase or lease spectrum licenses from other providers.

  Agency Affected: Federal Communications Commission

2.1.5. NTIA Broadband Programs across the United States:

The Department of Commerce (DOC) National Telecommunications and Information Administration (NTIA) provides key leadership in national and tribal broadband expansion. Literature review revealed that the NTIA has many articles and websites dedicated to the advancement and success of broadband network technology. There is a very active New Mexico state initiative regarding statewide broadband programs and when looking at the NTIA web site[5], it becomes apparent that current information is updated for every state in the United States regarding the advancements of broadband. Additionally, every state has a web site link on the map. It appears that National-Tribal broadband information is lacking.

2.1.5.1. NTIA 2.5 GHz Rural Tribal Window

The NTIA 2.5 GHz Rural Window is a unique opportunity for Tribes in rural areas to directly access unassigned spectrum over their Tribal lands, subject to buildout requirements. The 2.5 GHz band is suitable for both mobile coverage and fixed point-to-point uses and is currently used to provide broadband service by legacy educational licensees and commercial providers that lease the spectrum. Depending on tribal needs, it can play an important role in the deployment of broadband and other advanced communications services on AI/NA lands. Additional detailed information is available on the website below, including how to determine whether 2.5 GHz spectrum is available over specific AI/NA lands.

Any federally recognized Tribe or Alaska Native Village may apply for spectrum in the Rural Tribal Window. Consortia of federally recognized Tribes and/or Native Villages, or other entities controlled, and majority owned by such Tribes or consortiums, are also eligible to apply.

[5] https://broadbandusa.ntia.doc.gov/

The Rural Tribal Priority Window opened Monday, February 3, 2020, and closes on Monday, August 3, 2020 at 6PM EDT: https://www.fcc.gov/25-ghz-rural-tribal-window.

2.2. U.S. Government Adoption of IPv6

A March 2020 Memorandum for Heads of Executive Departments and Agencies: Completing the Transition to Internet Protocol Version 6 (IPv6), advocates the completion of USG adoption of IPv6 only. It States:

"Beginning in 2005, the Federal government's IPv6 initiative served as a vital catalyst, fostering commercial development and adoption of IPv6 technology. In the last 5 years, IPv6 momentum in industry has dramatically increased, with large IPv6 commercial deployments in many business sectors now driven by reducing cost, decreasing complexity, improving security and eliminating barriers to innovation in networked information systems. Several large network operators, software vendors, service providers, enterprises, state governments, and foreign governments have deployed significant IPv6 infrastructures. In fact, many of these organizations have migrated, or are planning to migrate, to "IPv6-only" infrastructures to reduce operational concerns associated with maintaining two distinct network infrastructures."

The same motivations apply to SLTT and private sector stakeholders, although an extraordinary benefit opportunity lies in new build areas, where disciplined baked-in security practices may be used from concept to disposition for a superior security posture.

It is important to note that RF and IP are tightly coupled in telecommunications networks and IT systems. An OT/IT/IoT discussion should encompass this RF/IP coupling and the congruent dependencies of scalable solutions with new standards, rather than isolated and separate technologies in the transport of information to fixed or mobile devices. Also needed is a recognition of the changing cyber ecosystem and the digital dichotomy that have significant impact to modernized and emergent ICS/SCADA systems.

3. CYBER INFRASTRUCTURE MODERNIZATION

3.1. Standards Based Technical Investments

Standards-based technical investments follow current standards. This is important as these newer standards support the vast expansion in connectivity and resultant next generation of advanced Internet services now and into the future.

Cyber innovation has high impact on community anchor institutions, including educational Internet access for homework and distance learning, as well as healthcare and telemedicine. Tribal/Pueblo regional broadband offers these and other opportunities.

Technical investments have been assessed based upon current standards-based technologies. These include IP and RF communications with a future forward investment posture due to a minimal investment in legacy standards and technology. This is relevant to new broadband and Internet service provider (ISP) development in heretofore unserved or underserved areas and tribal populations. Virtual services, such as Cloud service provider (CSP) adoption is also be considered.

3.1.1. Internet Protocol

Legacy and current IP versions are not interoperable. Each version actually comprises suites of related specifications and protocols.

- IPv6 from legacy IP, version 4 (IPv4)
- Neighbor discovery protocol (NDP) from address resolution protocol (ARP)
- Domain Name Service (DNS) IPv6 (quad-A) AAAA records from DNS IPv4 address (A) records

3.1.2. Radio Frequency

Legacy and current RF communications technologies are not interoperable.

- Fifth Generation (5G) new radio (NR) from 2G, 3G, and 4G mobile communications
- Project 25 (P-25) 700-800Mhz Digital Narrow Banding from Land Mobile Radio emergency communications

3.1.3. IPv6 and 5G NR

The two telecommunication standards are set to change the Internet posture now and into the future. Disruptive technology changes encompass IT, OT, Communications, and ICS/SCADA. The Internet Engineering Task Force (IETF) IPv6 specification (RFC 8200, July 2017), and the 3GPP 5G NR or 5G specification are being deployed on a worldwide scale. This means that older technologies are being displaced, which importantly offers an opportunity to build-in cybersecurity, physical security, and resilience as design requirements in modernization and security initiatives. Ultimately, successful protection of infrastructure and information will depend on understanding these new build technologies as foundations in the changing cyber-ecosystem.

Sustainability advantages can be realized by building securely in the early deployment of these new build technologies. Advantage can be gained through concept to disposition CPR design comprising cyber threat mitigation, physical threat mitigation, and resilient hazard mitigation as design requirements with criteria unique to each challenge and the task at hand. CPR design provides a distinct leap-ahead opportunity in heretofore unserved and underserved areas that have a historic under investment in older technologies. The benefit is a more secure and less rigorous transition to new technologies when compared to a forklift transition from legacy technologies.

The IPv6 standard was ratified in 1998 by the IETF and is a mature standard that has been Internet routable via Verisign, Inc. since 2008. New hardware and software are required because IPv6 is not backward compatible with IPv4. IPv4 simply cannot meet the expansive growth happening due to global broadband expansion and vast proliferation of IP enabled devices. The five regional internet registries have years ago exhausted the available address space of IPv4. Fortunately, products are mature and embedded IPv6 functionally is available in virtually all current systems. Unfortunately, worldwide IP dependence is in a state of IPv4 and IPv6 or dual-stack complexity.

A primary IP challenge becomes workforce knowledge skills and abilities development to manage two distinctly different and vastly different in scale IP versions. Further complicating the dual-stack issue is that many still refer to IP as one common transport layer technology, when in fact there are two incompatible versions. IPv6 supplants the dated IPv4 specification.

The 5G standard is a work in progress. 5G refers to the fifth generation of cellular mobile communications. Similarly, new hardware and software are required because 5G is not backward compatible with 3G/4G. 4G also does not meet global broadband needs in the vast proliferation of RF enabled devices. Fiber backhaul may be needed to reach small shorter distance cells that offer 5G millimeter (mm) Gigabit (30-300 GHz/10Gbps) throughput. Power drainage is a problem for 5G NR smartphones. Device energy storage and better power efficiencies are being developed and tested.

5G security will require new architectures and device functionality, such as Wireless Intrusion Protection Switching (WIPS) and proactive content caching at base stations. Quality of Service (QoS) and Quality of Experience (QoE) become important considerations in a combined 5G/IPv6 foundation, for example in dense population deployments, such as stadiums. There are caveats as 5G frequency ranges (FR1 - 450MHz-6GHz, FR2 - 24-52GHz) are more susceptible to interference.

RF and IP based mobility are inextricably linked, but it doesn't stop there. Accompanying standards and technologies that are associated with the changing cyber-ecosystem include:

- IETF IPv6
- 3GPP 5G NR
- IEEE 802.11ax (5.180-5.845 GHz), referred to as WiFi6, along with Orthogonal Frequency Division Multiplexing (802.11ax OFDMA), and Multiple Input Multiple Output antennae arrays, to support wireless devices outside of 5G channels
- Enhanced Mobile Broadband
- Ultra Reliable Low-Latency Communications
- Massive Machine Type Communications
- Software Defined Networks/Network Function Virtualization
- Software Defined Wide Area Networks
- Software Defined Radio
- TV White Space for communication transmission in between TV licensed channels (54-88 MHz, 170-216 MHz, and Wireless MIC 470-698 MHz) and the point-to-multipoint protocol
- IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), an Internet of Things (IoT) standard
- Virtualization and Digital Transformation including Cloud services, AR, VR, ML and AI

(Source: 5G World Alliance (5GWA)) "*The mission of the 5G World Alliance is to promote 5G as the Neutral Next Generation World Wide Wireless Internet by integrating new technologies with a holistic integrated approach combining IPv6-based Machine-to-Machine, Mobile Internet of Things, Mobile Cloud Computing, Software Defined Networks (SDN), Network Functions Virtualisation (NFV), Fringe Internet, Tactile Internet, focusing on commonly agreed requirements to garner support for seamless worldwide networking interoperability and spectrum harmonisation and foster coalition efforts to converge and focus the work for greater impact and exploitations for the common good.*"

"*5G is considered an all software and all distributed network*" former Chairman of the Federal Communications Commission and Brookings scholar Tom Wheeler

Use cases that drive accelerated 5G/IPv6 deployments include:

- Bridging the Energy Divide
    - IPv6 is necessary for addressing Distributed Energy Resource devices that are proliferating at an accelerated rate. Industry is already deploying Smart Grid, Smart Metering, and ICS/SCADA modernization (perhaps too rapidly as many still base network and communications design on legacy standards).

    - Wireless short-range communications such as 5G, Blue Tooth, and low power Blue Tooth will also aid in deployment of distributed ICS/SCADA sensor networks.
    - Energy ICS/SCADA security is a high area of impact
- Bridging the Digital Divide
    - IPv6 in a worldwide broadband expansion is essential for new service and device availability in unserved and underserved areas
    - 5G enhances broadband expansion worldwide, although 5G may not be appropriate for rural areas because of shorter distance coverages, it can be used with other wireless technologies.
    - Distance learning, telemedicine, and economic development in rural areas are areas of impact.
- Internet of Things
    - IPv6 enables address availability for vast device growth in the IoT
    - 5G wireless enables vast device growth and deployment of mobile devices that depend on lower power, low latency, and increased bandwidth/throughput in the IoT
    - IoT devices are estimated to be 20B by 2020, 60B by 2024. Such systems will require more deterministic operations that are dependent on lower latencies (>10ms)
    - The Industrial Internet of Things is emerging
    - The Mobile Internet of Things is emerging
    - Critical infrastructure resilience and manufacturing are areas of impact
- Automated Self-Driving Vehicles
    - New infrastructure and vehicles are needed, Dedicated Short Range Communications (DSRC) is being used in US proof of concept deployments. 5G and IPv6 are also enabling technologies.
    - Sensor instrumented infrastructure and vehicle-to-vehicle communications are areas of impact
- FirstNet
    - FirstNet is a National Public Safety Network. New functionality and mobile devices are needed to support first responders that will be enhanced by 5G and IPv6. Data validation is an important consideration so that first responders have accurate and timely information (low latency and high bandwidth).
    - Project-25 (P25) is an associated emergency communications technology, which facilitates a transition from older Land Mobile Radio (LMR) to newer 700/800Mhz digital narrow banding radio communications
    - 5G and P-25 are two examples of RF spectrum reallocation (similar to the TV Digital Dividend)
    - Emergency Services is an area of impact
- Critical Infrastructure Sectors
    - ICS/SCADA security need is increasing across all critical infrastructure sectors
    - IT, Communications, Energy, Agriculture, Water and Waste Water, and Transportation modernization are areas of impact
- Smart Cities
    - Smart cities will depend on 5G high bandwidth and low latency
    - Smart cities will depend on IPv6 vast IP address availability
    - Anchor institutions, such as healthcare, education, and law enforcement are areas of impact
- Virtualization
    - Cloud, Broadband, 5G, and IPv6 combine to serve new technology innovation and distributed rural connectivity and capabilities, in for example, critical safety and security OT systems

    - Large distributed industrial, IT, and OT systems can benefit from virtualized automation, for example AR/VR, ML and AI
    - Big Data analysis and information assurance are areas of impact
- Bridging the Digital Dichotomy
    - USG is in process of adopting IPv6 only
    - Scalable 5GNR and IPv6 standards adoption is necessary for unprecedented connectivity

In summary, the changing cyber-ecosystem technologies facilitate Internet and critical infrastructure modernization and security. Many new technologies are not backward compatible with older technologies. The changing technology landscape presents new risks at a time of worldwide transition to new technologies and continued dependence on old technologies. The tandem pursuits of next generation capability and reduced risk can be achieved by decommissioning old technology investments and moving solely to a new technology basis. The transition will take various levels of time, resources, and effort depending on the scope and maturity of organizational infrastructure readiness. Additionally, new technology innovation presents unprecedented high-impact CPR security and technological leap-ahead opportunities with broadband service expansion into unserved or underserved areas. These opportunities are of particular importance in critical infrastructure modernization, security, and resilience with essential benefits to critical infrastructure disruption response planning.

Key concerns are:

- Risk Management
- Cybersecurity
- Technology Investments
- Workforce Knowledge Skills and Abilities Development

Recommendations include:

- Consider a strategic approach to invest in current technology standards and security architectures
- Train the Science, Technology, Engineering, and Math (STEM) workforce for the new cyber-ecosystem
- Implement CPR design criteria for new software and infrastructure build initiatives
- Use the three cybersecurity tenets: Confidentiality, Integrity, and Availability (CIA) for IT in that given order, for example enterprise and CSP
- Use the three cybersecurity tenets for OT, for example ICS/SCADA, in the Availability, Integrity, and Confidentiality (AIC) given order of precedence
- Telecommunications security may be considered from an OT perspective, where an ISP provides service availability first (AIC), business operations should follow the CIA order of precedence
- Consider a data-centric security approach for virtualization initiatives, for example on-premises to off premises Cloud service transitions, when data is transferred from data-owner controlled infrastructure to data-steward controlled infrastructure

3.1.4. Virtual Technologies

Legacy and current virtual network and computing technologies are not interoperable by virtue of legacy client server versus virtual software defined deployment models, such as Cloud.

- Off-Prem Cloud service and workflow transition from On-Prem data centers
- Private Cloud
- Hybrid Cloud
- Public Cloud
- Software defined networks (SDN), Network function virtualization (NFV), and software defined radio from legacy enterprise network deployment
- Machine Learning
- Virtual Reality

- Augmented Reality
- Artificial Intelligence

A virtualized software defined future is replacing the technological past. The cyber critical infrastructure impacts are significantly increased connectivity and automation, facilitated by new technologies with additional vulnerabilities. This document endeavors to shed light on a path forward with a compressive review of the changing cyber-ecosystem.

Incompatible old/new sets of technologies are illustrated below.

Standard	Legacy Version	New Version	Impact
Internet Engineering Taskforce (IETF) Internet Protocol	IPv4	IPv6	Scalability and Address Availability
Third Generation Partnership Project (3GPP) Mobile Communications	2G, 3G, 4G	5G	Higher Density, Shorter Distance, Wireless Broadband
Institute of Electronic and Electrical Engineers (IEEE) 802.11	802.11 WiFi	802.11ax WiFi6	Wireless Communications outside of 5G
Association of Public-Safety Communications Officials (APCO) Project 25 Emergency Communications	Land Mobile Radio	P25 700-800Mhz Digital Narrow Banding	Digital Two-Way Radio with Encryption

Table 4. Non-Interoperable Technology Standards

3.1.5. Data Center and Environmental Controls

Data center environmental controls should include but not be limited to the following:

- Environmental conditions: Air temperature (supply and return), Humidity/Dewpoint, Water temperatures (supply, return/refrigerant monitoring, metering on systems to gather data.
- Power – submetering for all IT infrastructure with separate metering for mechanical support systems to collect data for PUE and power utilization.
- Climate metrics – Metering and data collection to utilize and manage environmental conditions

Many of these data points will lead to a programmatic response to enhance the capabilities to operate the data center at the optimum curves to work toward a self-sustaining data center along with the capabilities to utilize renewables and with a known reliable system.

Classic computing and High-Performance Computing (HPC) facilities pertain to the aforementioned data center and environmental controls. HPC systems may also serve as capable platforms for cybersecurity research including behavioral, anomalistic, and artificial intelligence development. For example:

- Large networks can be viewed as complex systems exhibiting emergent behavior. Without a more profound understanding of these complex systems and their behavior it is difficult to learn how to protect them. HPC can provide a platform for simulation of large-scale networks and discovery of their behaviors.
- Deep packet inspection requires high-speed pattern matching on large datasets and, if implemented with sufficient throughput, could be used for effective intrusion detection, prevention, and filtering of http traffic.

- Large-scale computation is needed for analysis of vast amounts of cybersecurity data collected across a wide area over time. HPC systems offer a means for large-scale computational capacity and management. In tandem, high-speed sensor networks offer a means of collection across a wide area over time.
- Correlation and analysis algorithms for wide area cybersecurity applications are lacking. Development of these algorithms is necessary to collect, transport, store, and conduct high performance analysis of cybersecurity data.

3.1.6. Cloud Services

Cloud services have displaced the need for large data center facilities. Such virtualization is still evolving and illustrated below.

Term	Definition
Infrastructure as a Service (IaaS)	The capability provided to the subscriber is to provision processing, storage, networks, and other fundamental computing resources where the subscriber is able to deploy and run arbitrary software, which can include operating systems and applications. The subscriber does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) (NIST SP 800-145).
Personal Identity Verification (PIV)	A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV requirements are defined in FIPS PUB 201.
Platform as a Service (PaaS)	The capability provided to the subscriber is to deploy onto the cloud infrastructure subscriber-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The subscriber does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment (NIST SP 800-145).
Software as a Service (SaaS)	The capability provided to the subscriber is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The subscriber does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings (NIST SP 800-145).

Table 5. Cloud Service Terms and Definitions

Cloud computing architectures shift responsibilities for provisioning of data and capabilities: Within traditional On-Prem computing architectures, organizations typically have data ownership and full control over the data collected and data-collection capabilities used in the context of information management and protection. However, Off-Prem cloud computing transfers a degree of responsibility to CSP, who serve as data stewards and sources for customer tenant cloud-based assets.

Data from cloud architectures is most relevant to Information Security Management: Cloud services abstract asset-based protections into a data-centric scheme, more wholly focused on an information "attack profile" and operational considerations. This abstraction, in turn, presents difficulties in extracting cloud-based Asset Management and Identity, Credential, and Access Management (ICAM) data from cloud architectures.

Data access and security changes with the adoption of cloud services, as the CSP owns and operates the hardware, while tenant data resides in data centers shared by other customers. The shared nature of cloud services creates a

challenge for collection and analysis of asset management data, which further impacts the security posture and situational awareness of the tenant organization. The attack surface, or exposure of a system to an attacker, can be bound by the aggregation of those assets and their use in a given environment. In other words, a protection level of information is based on the data value or sensitivity to an organization, and conversely to an adversary. A low, moderate, or high value/protection key pair can be used to assess a specific protection posture needed for a given data asset.

3.2. Wide Area Broadband Network Design

Wide-area broadband network design for Tribal/Pueblo communities is a new-build opportunity. There are different ways to consider design options: 1) build with well-known although legacy technologies for faster deployment; 2) built with current standards-based technologies for a long-term advantage; 3) build with both legacy and current standards-based technologies, which complicates design, deployment, maintenance, and operations.

- Option 1 is a default for many organizations due to common knowledge and a high technical comfort level for many cybersecurity, system, and network professionals. Option 1 risk includes a high of dependency on legacy technologies that cannot scale to growth of new connectivity.
- Option 2 requires building a knowledgeable workforce along with a security focused design practice. Technological risks remain but can be better managed with security as a set of design requirements.
- Option 3 adds a built-in and inherent dependency on older technologies that carries mortgages into the future, which include support and eventual transition to newer technologies.

The overall goal for stakeholders is the eventual migration to current technologies and away from legacy technologies and overhead. Therefore, *Option 2 is the recommended path forward for secure and resilient regional broadband and critical infrastructure digital transformation.*

3.2.1. Secure and Resilient Broadband Big Picture

Broadband is expanding worldwide and is a national priority as illustrated by the Networking and Information Technology Research and Development (NITRD) Program Broadband Resource Guide below:

Source: Networking and Information Technology Research and Development Program, https://www.nitrd.gov/apps/broadband/

Figure 16. NITRD: Broadband Resource Guide

The IT and Communications critical infrastructure sectors are focal points that encompass a larger cyber-innovation nisus with momentous impact on other critical infrastructure sectors. The national critical infrastructure fabric comprises federal, state, tribal, local, and private sectors stakeholders. Our focus herein is strategic benefit National-Tribal CIP.

Figure 17. DHS Critical Infrastructure Sectors

Cyber innovation originates in the IT and Communications critical infrastructure sectors, which has impacts that span all other critical infrastructure sectors. This is demonstrated by the new ICT standards and worldwide broadband expansion. The modernization of ICS and SCADA systems includes smart-grid, microgrids, and smart-metering. Note that the OT Energy Field Area Network (FAN) common reference model illustrated below is very similar to an IT protocol stack.

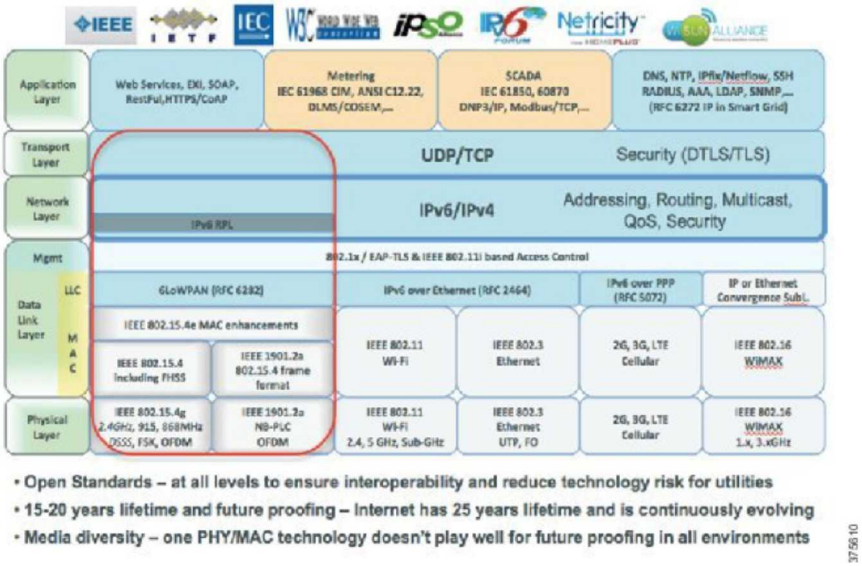


Figure 18. Energy Field Area Network Common Reference Architecture

The FAN diagram illustrates examples of IEC Common Information Models (CIM). CIM are a product of the DMTF (formerly known as the Distributed Management Task Force), which creates open manageability standards spanning diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage: https://www.dmtf.org/. CIM are abstract, hierarchical representations of complex systems. The utility of CIM are relevant in policy based network management, the Energy FAN, and subsequently could be valuable in Cloud computing and critical infrastructure definition of complex distributed systems, attributes, and metrics.

3.3. Design Assurance

Topics that will be addressed in this section, as they pertain to the Design Assurance phase of a telecommunication's critical infrastructure plan.

3.3.1. Planning & Design Phase

1. Physical Security Policies and Access Control Procedures
2. Enterprise Information Security Policy (EISP)
3. Issue-Specific Security Policy (ISSP)
4. System-Specific Security Policy (SysSP)
5. ISO 2700 Series
6. NIST Security Models

3.3.2. Design & Implementation Phase

1. Physical Security Controls
2. Securing Local Area Networks (LANs)
3. Securing Wide Area Networks (WANs) and Wireless Access Points
4. Internal Monitoring Capabilities

3.3.3. Review/Post-Implementation Phase

1. Security Documentation Review
2. Log Review
3. Ruleset Review
4. System Configuration Review

It should be noted that The Planning & Design Phase and the Design & Implementation Phase are not mutually exclusive; in fact, they depend on each other greatly. The Planning & Design Phase is used to help guide the Design & Implementation Phase, but it is not a static process. Changes are likely to happen depending on obstacles encountered during the Design & Implementation Phase. For instance, during the Planning & Design Phase an organization gathers documents, establishes requirements, and chooses the methods and procedures most applicable to the given situation. During the Design & Implementation Phase said organization physically attempts to implement the design choices that were established during the Planning & Design Phase.

3.4. Physical Security Policies and Access Control Procedures

Physical security is the first line of defense against cyber-attacks and should never be overlooked. Recent research suggests that nearly half of all successful cyber-related attacks occurred because of weak, or nonexistent, physical security barriers.

There are numerous policy manuals available on the Internet; however, it is advised to follow ISO 17799 (Section 7: Physical and Environmental Security) and ASIS Internationals Enterprise Security Risk Management (ESRI) guidelines. Some of the key takeaways available in both documents are listed below:

- Determine the need for armed/unarmed security personnel
- Recommended to install intrusion (burglary) alarms with backup power systems and third-party monitoring services
- Implement redundant power systems, especially for communications and alarm systems.
- Install access control devices, like card readers and biometric scanners, locked doors (it's common for attackers to find open doors), and segment facilities for restricted areas with enhanced security controls (i.e. server rooms). NOTE: Radio Frequency Identification Devices (RFID) are good access control devices but be aware some attackers can use RFID readers. It is suggested that all RFID's are shielded with a few sheets of aluminum foil or encased in a RF shield; however, contrary to popular belief RFID hacking is very rare. Because it CAN be done, it should at least be taken into consideration.

- Using best practices like securing routers in locked server rooms so they can't be reset to factory settings or physically damaged.
- Implementing controls to limit or prevent tailgating with the use of mantraps. A mantrap is any area that has two independent entry points, where one does not open until the other has closed. For example: entry into a parking lot is controlled by a garage with two doors, one that opens to the exterior portion of a compound and one that opens to the interior portion of the compound. The interior door will not open until the exterior door has fully closed. The garage space is large enough for only one car, so tailgating is effectively eliminated.
- Implementing remote wiping procedures for stolen equipment, like laptops and company issued mobile devices.
- Cable locks for servers, hard drive ports, or any other device that contains critical data.
- Closed Circuit Television (CCTV), possibly equipped with image recognition capabilities (to recognize if a person is carrying a firearm, for instance)
- Legal Personnel to help draft policies concerning Use of Force, investigations, and so on.
- Methods to detect false fire alarms triggered by an attacker.
- Physical construction materials. For example: can an attacker break a window at night with a simple window punch (not usually possible with impact glass), smash a hole in a concrete wall with a sledgehammer, or drive through a weak perimeter gate
- Exterior AND interior perimeters.
- Proper lighting at night to avoid "black-out spaces," both within and along the perimeter of a facility
- Motion detection devices. Should be placed on the perimeter and interior of Data Centers, SOC/NOC facilities, power facilities, etc.
- Metal detectors and/or X-ray machines, if feasible
- Protect network cabling, underground if possible, using Raceway (aka conduit). Secure wiring closets and junction boxes with access control devices and security alarms.
- Properly vetted personnel. Unfortunately, insider threats are real and can be very damaging to a company/organization.

3.4.1. Enterprise Information Security Policy

Also known as a general security policy or IT security policy, EISP directly supports the mission, vision, and direction of an organization. This is an executive-level document, usually drafted by the Chief Information Officer. The EISP should remain relatively static, unless new technologies are introduced in the network architecture. The EISP defines the purpose, scope, constraints, and applicability of the security program in the organization. The EISP also addresses legal compliance standards. An EISP typically involves the following components:

- Statement of Purpose
    - Answers the question, "What is the policy for?"
    - Identifies the elements of a good security policy
    - Explain the need for information security
    - Specify the various categories of information security
    - Identify the information security responsibilities and roles
    - Identify appropriate levels of security through standards and guidelines
- Information Technology Security Elements
    - Defines Information Security
    - Lays out security definitions or philosophies
- Need for Information Technology Security
    - Provide information on the importance of information security in the organization and the obligation to protect critical information about customers, employees, and markets
- Information Technology Security Responsibility and Roles
    - Defines the organizations structure designed to support information security.
    - Lists individuals and their respective responsibilities within the organization
- Reference to Other Information Technology Standards and Guidelines

3.4.2. Issue-Specific Security Policy

The ISSP instructs employees on the proper use of technologies and processes, to include:

- Use of company-owned networks and the Internet
- Use of telecommunications technologies (fax, phone, VoIP, etc)
- Use of email
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibition against hacking or testing organization security controls, unless authorized for internal or external testing.
- Home use of company-owned computer equipment
- Use of personal equipment on company networks
- Use of photocopy equipment, including cameras.
- Limiting what types of technology can accompany an employee or visitor. i.e. no cell phones, USBs, or other electronic media, including anything equipped with Wi-Fi or Bluetooth, into limited access areas.

An ISSP typically has the following components:

- Statement of Policy
- Authorized access and usage
- Prohibited usage
- Systems management
- Violation of policy
- Policy review and modifications (see section C for additional information)
- Limitations of liability

3.4.3. System-Specific Security Policy

SysSPs can be separated into two different categories, Managerial Guidance SysSPs and Technical Specifications SysSPs. The difference between each document lies in the technical details. Managerial Guidance SysSPs are intended for managers to help regulate the behavior of people in the organization and to provide guidelines that must be followed, while the Technical Specifications SysSP provides procedures on how to implement certain technologies. For instance, the Technical Specification SysSps might contain the procedures for implementing a firewall but said configurations must follow the guidelines (or the bounds) set forth in the Managerial SysSp. It should be noted there are two general methods for implementing technical controls: Access control lists (ACL) and Configuration rule policies.

3.4.3.1. ISO 2700 Series

The International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC) [ISO/IEC 17799] is an international standard framework for information security. ISO 17799 was renumbered in 2007 to ISO 27002. The standard structure and organization of ISO 27002 is as follows:

1. Risk Assessment and Treatment
2. Security Policy
3. Organization of Information Security
4. Asset Management
5. Human Resource Security
6. Physical and Environmental Security
7. Communications and Operations
8. Access Controls
9. Information Systems Acquisitions, Development, and Maintenance
10. Information Security Incident Management
11. Business Continuity Management
12. Compliance

The following infographic describes the process to set up an information security management system based on the ISO 27002 methodology:

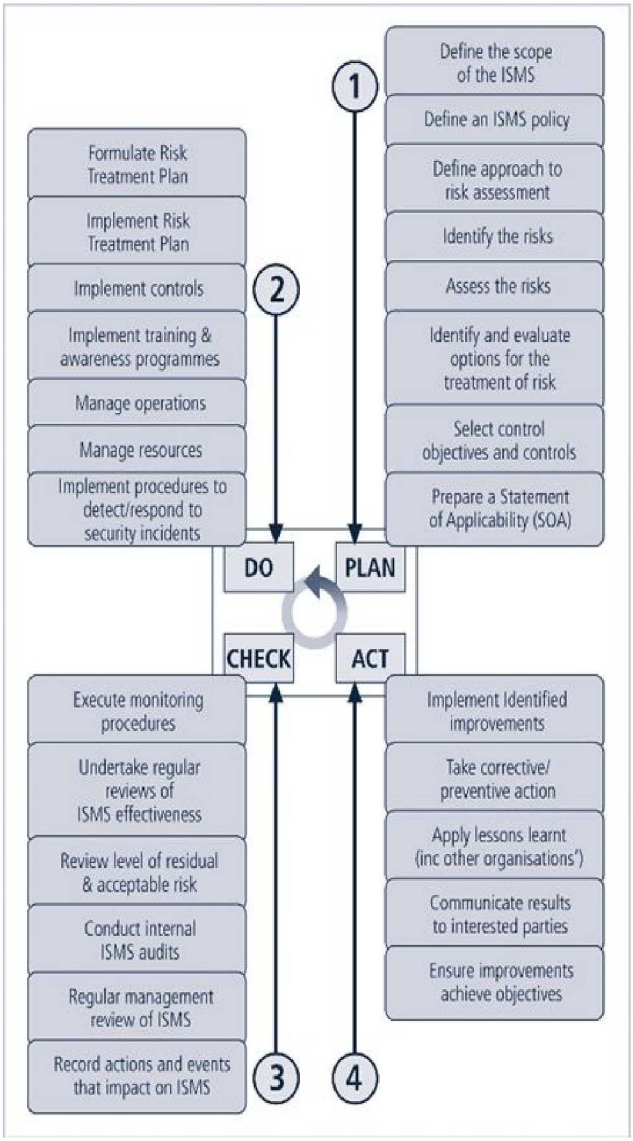


Figure 19. ISO 27002 Information Security Management Methodology

3.5. NIST Security Models

The Computer Security Resource Center of the NIST provides several documents that can be used to create an information security framework. The following NIST documents should be consulted during the planning phase:

- SP 800-12: *An Introduction to Computer Security: The NIST Handbook*
- SP 800-14: *Generally Accepted Security Principles and Practices for Securing Information Technology Systems*
- SP 800-18 Rev. 1: *Guide for Developing Security Plans for Federal Information Systems*
- SP 800-30: *Risk Management Guide for Information Technology Systems*
- SP 800-53 Rev. 3: *Recommended Security Controls for Federal Information Systems and Organizations*

Discussed below are additional things to consider when developing an information security plan:

- Define rules for good password management among employees and executives alike (i.e. length and type of characters to be used, when to change passwords, where NOT to store them, etc.). This information should be well-defined in the security policy manuals.
- Define reporting procedures when incidents occur, or suspected violations have been discovered (internal and external), including what disciplinary actions will be taken if said procedures are not followed.
- Document incident response procedures, including timelines, the designation of trained personnel who can respond to the scene, and/or the name and contact numbers of an external incident response team.
- Fully examine the NIST documents and the ISO 27002 Standards
- Understand the "Defense-in-Depth" model, which follows a layered approach to security. Defense in Depth is comprised of the following core philosophies: redundancy, security perimeters, and security domains. The following diagram illustrates the concept of Defense in Depth:

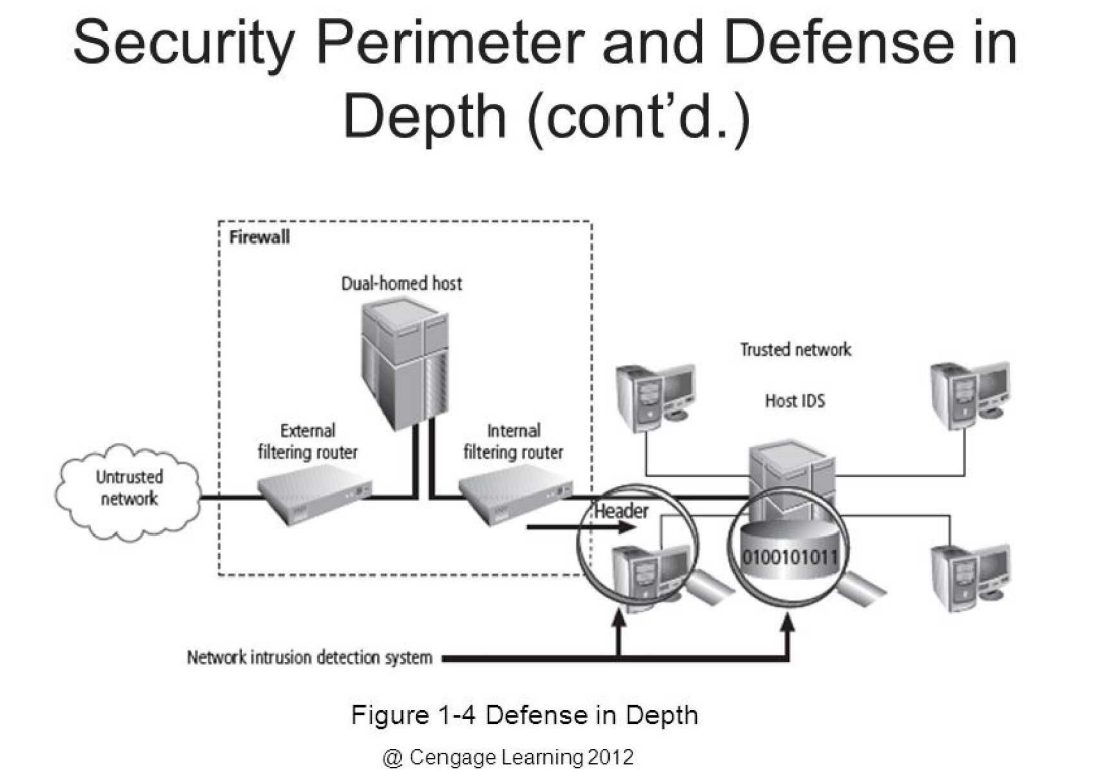


Figure 20. Security Perimeter and Defense in Depth [excerpted]

Source: Guide to Firewalls and VPN's, 3rd Edition, Section B – IMPLEMENTATION & DESIGN PHASE.

NOTE: Items in green are direct commands that should be typed in Windows Command Prompt, PowerShell, or the Linux Shell/Terminal.

3.5.1. Securing Local Area Networks(s) / Physical Network Settings

Before implementing a secure local area network, please consult the security policies and planning documents established in the Planning & Design Phase. Additionally, a realistic assessment of the risks and resources available should be made before committing to any physical implementations. Some of the typical challenges associated with a network design include the following:

- Securing the network from internal attacks
- Securing web servers and pages, DNS, and mail servers
- Securing personally identifiable identification (PII), sensitive and mission critical internal resources, customer databases, and trade secrets
- Building a framework for administrators, managers, and technical personnel to effectively manage and secure the network, including the ability to recover data (RAIDs, incident response, digital forensics, etc.)

Creating a secure LAN typically consists of the following components:

Topology and Architecture: The network topology is the physical layout of the network. For instance, a topological design needs to consider how the network will be distributed to buildings and offices, how users will access the network, how remote users will connect to the network, fiber optic lines, telephone lines. Physical topologies also consider the location and connections associated with routers and switches. A logical topology (typically Layer 3) describes the interconnectivity of the network, especially with respect to virtualization, like VLANS and VPNs. The following infographic illustrates the differences between logical and physical topologies:

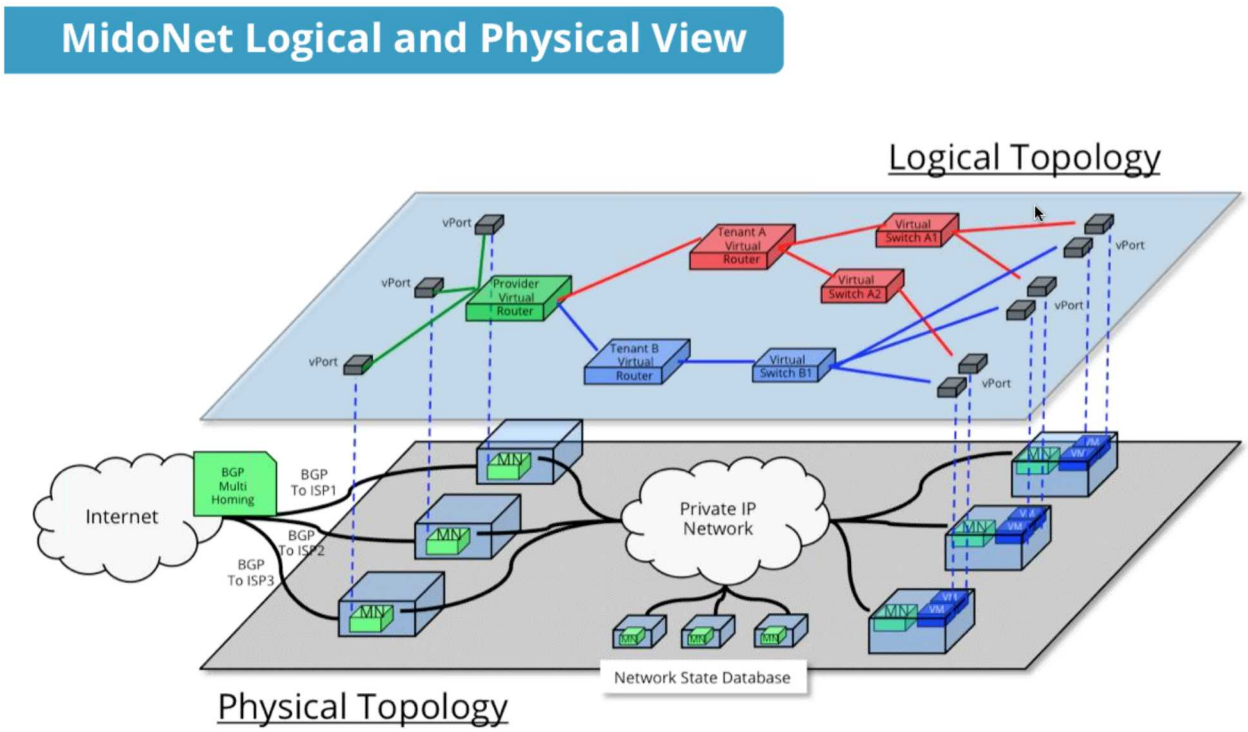


Figure 21. Physical/Logical Topologies

Securing Routers and Switches: Most networks will require some type of subnetting, especially where security is concerned. By implementing routing at the network core, segments can be isolated into broadcast domains. This helps reduce sniffing or ARP based attacks between segments. Within each subnet the hosts should be connected to an ethernet switch. Hubs can be used as well, but they do not provide CSMA with collision avoidance so they are generally not recommended.

Layer 3 Design and Access Lists: Because the technical specifications for the layer 3 design should have been created during the Planning & Design Phase, you can use access lists at Layer 3 to implement the security policy. During this portion of the implementation phase only permitted packets will be allowed into the network. All outgoing traffic should be filtered to eliminate spoofing and minimize malicious activity, including connections to dangerous websites or shared resources. Additionally, traffic leaving each subnet should be filtered to prevent spoofing.

Securing Layer 3: Secure management of routers is essential to ensuring a network remains secure. There are several mechanisms by which this can be done, such as creating a management VLAN, creating access lists on the management ports to block illegitimate connections, Out of Band (OOB) communication, using strong authentication provided by a one-time password server, using encrypted communication protocols like SSH (never telnet), and logging to the syslog servers located on the management network.

Layer 2 Design: VLANs should be configured per switch to help minimize the chance of an attacker moving from one VLAN to another. Implement physical security to switches, such as locking them inside limited access rooms and disabling unused ports. Users should be required to authenticate using LDAP or some other mechanism like RADIUS. It is also advised to limit MAC addresses to only those permitted to communicate on the open ports. This can be done with the use of static or secure MAC assignments.

Additional security suggestions are as follows:

- Implement intrusion detection systems (IDS)
- Private VLANs and VLAN ACLs
- Micro VLANs
- IPSEC or Ip Security techniques, which ensures that every packet transmitted on the network LAN uses strong encryption algorithms.

Additional resources can be found in the NIST SP-800 series documents, from ISO 27002, and SANS.org.

3.5.2. Securing Wide Area Networks / Wireless Access Settings

Most of the guidelines presented in Securing Local Area Networks also apply to Wireless Networks, including susceptibilities. The key difference between the two transmission types is that wireless communication signals are transmitted without physical media. Instead, wireless communication uses radiated signals, like radio frequency, light, or some other part of the electromagnetic spectrum. For instance, Wifi 802.11a/b/g/n typically uses the ~2.4GHz range, which is part of the Ultra High Frequency range or UHF. 802.11/ac operates at ~5GHz and fluctuates between UHF and Super High Frequency (SHF). 5G, on the other hand, is intended to use the SHF frequency band, while teetering on the Extremely High Frequency band (EHF), which is also known as millimeter wave. SHF ranges from 3GHz – 30 GHz, while EHF ranges from 30 GHz to 300 GHz. UHF, SHF, and EHF are all part of the radio spectrum.

When implementing a wireless infrastructure, it is advised to consult the security policy manuals created during the Planning & Design Phase. However, the following points of information should be addressed at some point during the Implementation Phase:

- DO NOT disable identifier broadcasting. Apple wireless calls this "creating a closed network". It is generally not suggested to hide the broadcast SSID, because attackers can easily find this information, and a hidden SSID suggests the network contains sensitive data. For example, the Windows command line to discover a hidden SSID is:
  - netsh wlan show networks mode = bssid
- Encrypt traffic passing between wireless devices using either WPA2 or WPA3. DO NOT use WPA or WEP. The following cryptographic mechanisms are as follows:
  - WPA3 – newest technology but likely the best
  - WPA2 – very good current technology that uses AES (Advanced Encryption Standard). Should be used with the Enterprise Model, which establishes a set of credentials for each device attempting to access the network.
  - WPA – very basic and should not be used
  - WEP – should never be used
- Change default passwords on routers and any other access points. This is a very common security mistake.
- Disable file sharing or, if absolutely needed, set up a dedicated directory for file sharing. Use password protection. In fact, you can password protect the entire directory. Never open an entire hard drive for sharing.
- Patch and update access point software
- Either disable or limit ad-hoc connections

- Employ the use of a VPN for very sensitive connections
- Employ a DMZ (Demilitarized Zone)

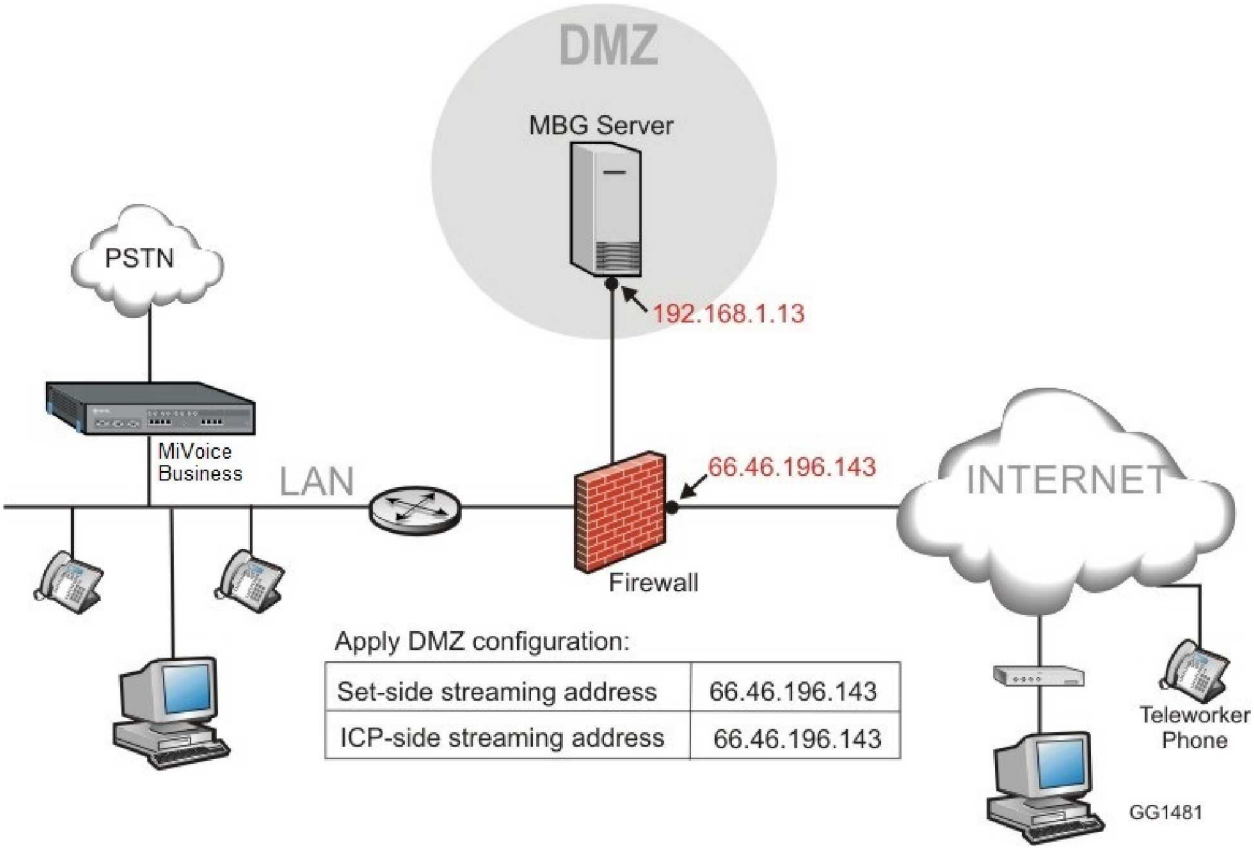


Figure 22. Demilitarized Zone Example

- Employ a honeypot
- Use external and internal firewalls
- Use edge routers in combination with firewalls and VPNs
- Prevent successful wardriving by implementing MAC filters, employ VPNs, encrypt data transmissions, change default wireless access-point passwords, and deploy external and internal firewalls with edge routing designs. Again, DO NOT disable broadcast SSID. This is an advisable technique to use for home networks but not for enterprise networks.

Network Sniffing:

- Establish Network sniffers at the following locations:
  - At the perimeter to monitor traffic entering and exiting the network
  - Behind Firewalls
  - Behind IDS/IPS (Intrusion Detection Systems and Intrusion Prevention Systems)
  - In front of a critical system or application
  - On a specific network segment, to validate encrypted protocols

File Integrity Checking:

- Can be accomplished with the use of a checksum protocol, which can be recomputed on a regular basis to detect alterations.
- Commercial host-based IDS's often come with this feature natively.
- Custom checksums can be implemented via scripting, commercial products, Linux based console commands (echo -n putorius | md5sum), Linux based packages like Advanced Intrusion Detection

Environment (AIDE), or Windows System File Checker (sfc /scannow), which can be accessed from the command prompt.

3.5.3. Internal Monitoring Capabilities

- Blue teams are entrusted with hardening network security
- Red teams are charged with attempting to defeat network security settings/protocols
- Both teams work together, never against each other

If feasible, consider creating a Network Operations Center and a Security Operations Center. Typically, the NOC and SOC have different roles in an enterprise environment. NOCs focus on availability and performance while SOCs focus on protecting intellectual property and customer data. There is a bit of overlap concerning the skillsets required to work in a NOC or a SOC, but it is generally agreed that advanced network engineers with specialized security training are needed to operate Security Operations Centers. In other words, many SOC analysts began their careers by working in a NOC.

SECTION C – DOCUMENTS REVIEW PHASE.

3.5.3.1. Log Review

- Establish well-defined logging rules. For example: all authentication attempts to critical servers should be logged.
- Back up log files remotely to avoid attackers deleting or altering log files
- System and service startup and shutdown information, installation of unauthorized software, etc
- Logs can show outbound and inbound connections/attempts
- Account changes, use of privileges, and application/database information
- patch management and IDS may record information on known vulnerabilities
- There are several methods in Windows and Linux to disable USB storage; however, it is also important to ensure USB devices have not been used to remove sensitive data. In Windows this can be done via the USBStor registry. In Linux you can use the commands lsusb and dmesg.
- NOTE: use automated tools and/or scripts to parse, filter, and organize data. Automated tools greatly reduce the time network admins spend on log reviews and maintenance.

3.5.3.2. Ruleset Review

- Network and host-based firewall and Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS).
  - Enforce least privilege, i.e. IP addresses for IPv4 and IPv6 and ports
  - closing all unnecessary ports
  - rule does not accidentally bypass other security rules
  - Be aware of false positives due to unnecessary signatures
  - Be aware of necessary signatures and update IDS/IPS regularly
- Router access control lists
  - Only route authorized traffic, drop everything else
  - REJECT internal traffic that is not authorized and DROP everything else. Rejecting external traffic immediately tells an attacker that the port is closed, but it also prevents them from flooding the network with multiple scans, so it is advised to DROP external traffic instead.
- Packet forwarding and rejection
- system events (stopping or allowing)
- creating incident alerts

3.5.3.3. System Configuration Review

- Adhere to the Security Content Automation Protocol (SCAP) for automated vulnerability management. SCAP is FISMA and NIST SP 800-53A compliant for security control testing.

- Automated checks can be used to determine such things as: improper security control configurations, unnecessary services and applications, improper users (names and permissions), passwords, privilege rights, logging and backup settings, etc. Security configuration files can be found in Windows Security Policy and in the /etc directory in Unix based architectures.

3.5.3.4. Periodic Penetration Tests/Vulnerability Assessments from Independent Companies/Organizations

- It is important to conduct external penetration tests to determine your networks security posture. There are several types of metrics associated with an assessment:
  - Attack-based
  - Vulnerability-based
  - Consequence-based
  - Adversary-based
  - Protection-based
  - Threat-based
- An assessment can include one or more of the metrics listed above.
- There are also several types of penetration tests:
  - Network Services
  - Web Application Tests
  - Client-Side tests
  - Wireless Network Tests
  - Social Engineering Tests
  - Black box, gray box, and White Box tests
    - Black box tests assume the assessor(s) have no internal knowledge of the target system. This closely resembles the processes and techniques a hacker or group of hackers would use to compromise a system or network.
    - Gray Box tests assume the assessor has some knowledge of the system, typically at the user level or at a slightly elevated privilege.
    - White Box tests are unique since they provide the assessment team with all information needed for a comprehensive assessment. This may include such things as source code, network diagrams, admin rights, and so on. White Box testing is especially useful during the design assurance phase.
      - NOTE: Black box and Gray box testing can damage networks, web applications, and systems depending on the nature of the attack, so it is advised to develop a comprehensive Rules of Engagement (ROE) document outlining what IS and IS NOT in scope for the assessment.

Example of an External Read Team:

Sandia Lab's IDART is a NIST-recognized method in SP800-115, Technical Guide to Information Security Testing. The method has been improved over time to help sponsors better assess and understand risks presented by a spectrum of adversaries. It supports repeatable assessments with measurable results that can be used to make improvements and evaluate progress. Sandia Lab's red teams perform IDART assessments to help stakeholders acquire an independent, objective view of system weaknesses using a range of adversary perspectives. Besides assessment planning and reporting of results, core IDART assessment tasks include:

- Characterizing the target system and its architecture
- Identifying nightmare consequences
- Analyzing the system for its security strengths and weaknesses
- Identifying potential vulnerabilities whose exploitation will result in nightmare consequences, and
- Providing prioritized mitigation strategies so owners can make risk-informed choices

<https://idart.sandia.gov/_assets/documents/IDART-Factsheet-v1.0.pdf>

3.6. Training

Training should never be overlooked when it comes to cybersecurity. There are numerous training institutions, like SANS and ISC^2, but it is also highly suggested to create an in-house training program.

Technical certifications can be costly and do not always ensure an employee /candidate has the necessary skills to perform satisfactorily; however, the following certs are generally well respected in the cybersecurity community and provide at least some measure of an individual's KSAs:

- CCNA - Certified Cisco Network Associate (intermediate level)
- CCNP – Certified Cisco Network Professional (expert level)
- MCSP/MCSE – Microsoft Certified Solutions Professional/Expert
- RHCSA – Red Hat Certified Systems Administrator
- CISSP – Certified Information Security Systems Professional (management level)
- GPEN - GIAC Penetration Tester
- GXPN – GIAC Exploit Researcher and Advanced Penetration Tester
- OSCP – Offensive Security Certified Pen-tester (very difficult and quite advanced)
- GCIH – GIAC Certified Incident Handler
- CFCE/CCE – Certified Forensic Computer Examiner & Certified Computer Examiner (device and network forensics training)

The GIAC certifications are associated with the SANS corporation, which is arguably the leading IT/Security training institute in the world. SANS certifications are accepted by the DOE, DOD, DHS, and the intelligence community. However, certifications should not be the only criteria established to help vet qualified personnel; in fact, many of the skills needed to perform IT and cybersecurity operations can be learned through independent self-study. For this reason, degrees are typically more relevant than certifications; however, a combination of education, self-study, and certifications is advisable. Strong candidates should even be given time after their hire date to obtain some of the certifications, rather than requiring all candidates have said certs before applying for the position. A well-defined training program might even provide study time for employees.

NOTE: Because IT/Cybersecurity is an ever-changing landscape, continued education is an absolute necessity.

A Design Assurance critical infrastructure plan will be forward focused in the modernized cyber ecosystem.

Illustrated below is a 100-year pictorial representation of the cyber ecosystem digital dichotomy. The first 50-years of Internet are based on older standards and technologies that cannot scale to today's needs; and the next 50-years will be based on newer scalable standards and technologies. The key takeaways are that training and technical investments are essential in the new technological paradigm.

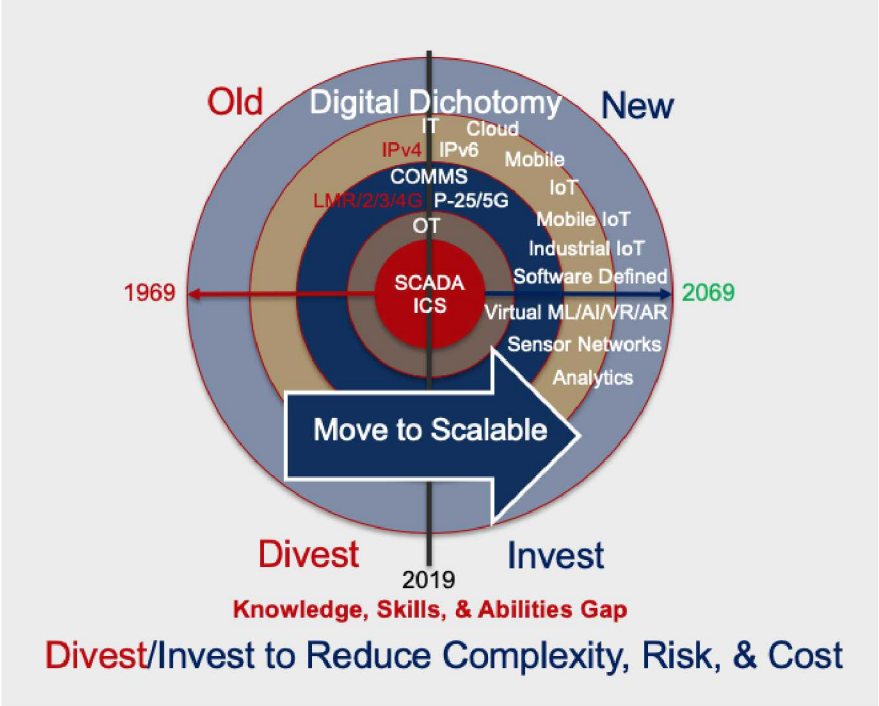


Figure 23. 100-Years Perspective of the Digital Dichotomy

An advantage of reduced attack surface threat exposure can be gained by moving to a single set of IP standards. For example, when IPv4 was predominant and prior to the address exhaustion in September 2015, one could argue that adopting IPv6 would add complexity, risk, and cost, so many chose to delay adoption. Conversely, now that IPv6 is embedded in all modern systems and fixed or mobile networks, the same logic applies in reverse: move to IPv6 only and divest in IPv4 to reduce complexity, risk, and cost. Similarly, a digital dichotomy exists for radio frequency communications technologies as well. Reinforcing the point that training is essential to gain a qualified workforce.

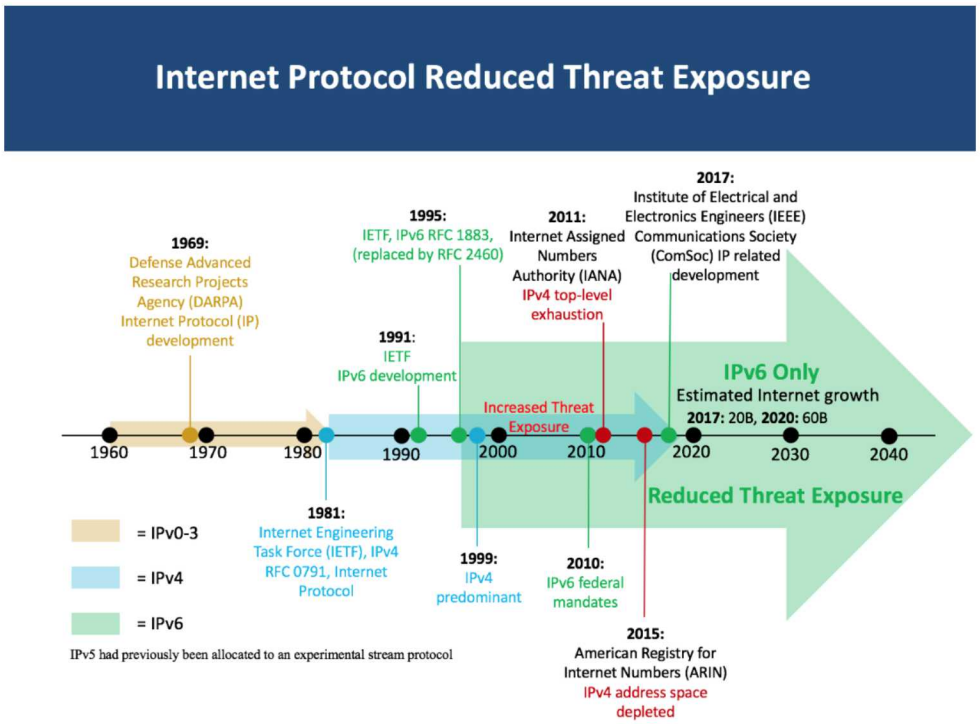


Figure 24. Internet Protocol Threat Reduction toward a Single Standard

4. RISK MANAGEMENT

Risk management is comprised of many facets. One perspective is cybersecurity, which implies an attacker/defender set of actions in the effort to protect information assets. An attacker defender timeline relating to cyber-relevant time (CRT) to respond and recover from disruptive cybersecurity events.

Cybersecurity is based on three tenets: Confidentiality, Availability, and Integrity. Confidentiality can be viewed as encrypted data at rest, in process, and in transit. Availability can be viewed in two ways – readily available and accessible information services; and readily available information itself. Integrity can be viewed as the right information at the right time to the right person, such that data is received as it was sent as intended without modification. These principals apply to On-Prem local area networks (LAN), Off-Prem Cloud services, and for mobile communications alike. Note that mobile communications are based on both RF and IP technology suites.

4.1. The NIST Special Publication 800-37, Revision 2

The NIST Risk Management Framework (RMF) illustrates an organization-wide risk management approach at three levels: Organization; Mission/Business Process; and Information System.

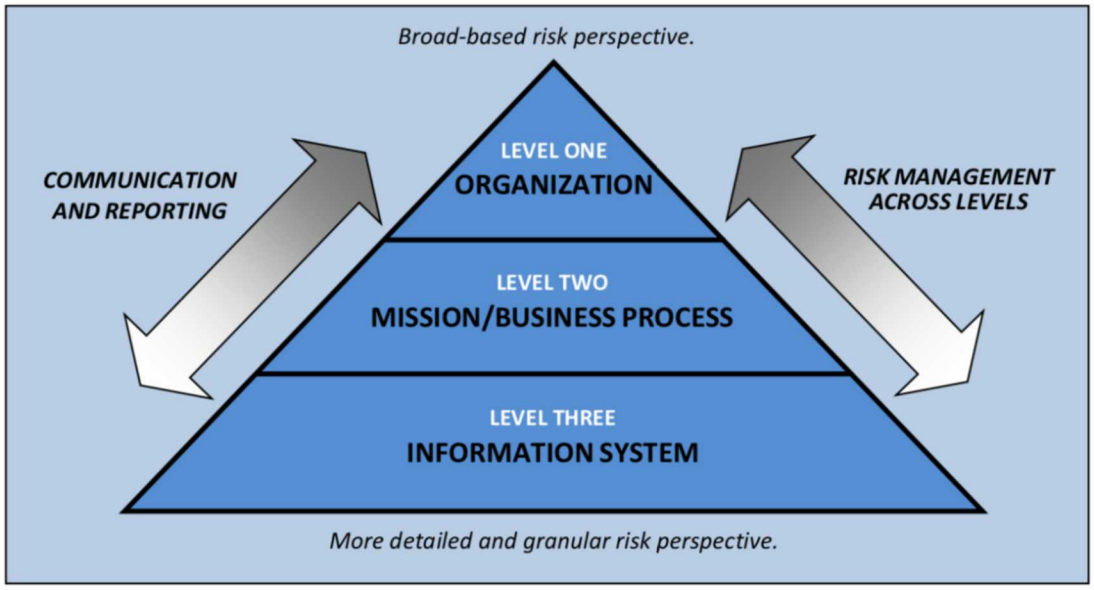


Figure 25. NIST RMF Organization-Wide Risk Management Approach

Inter-organizational or multi-organizational risk management is the concern in wide-area shared critical infrastructures. This is the case with multi-stakeholder facilities within a critical infrastructure sector or interdependencies across sectors. Consequently, large distributed critical infrastructure systems may have a complex of multiple data owners and data stewards and information asset values, which accompanies multiple organizational sets of roles and responsibilities.

Each authoritative organization should locally administer the risk management tasks, illustrated below, and subsequently coordinate the Identify, Protect, Detect, Respond, and Recover functions for data-centric protection of information across relevant organizations.

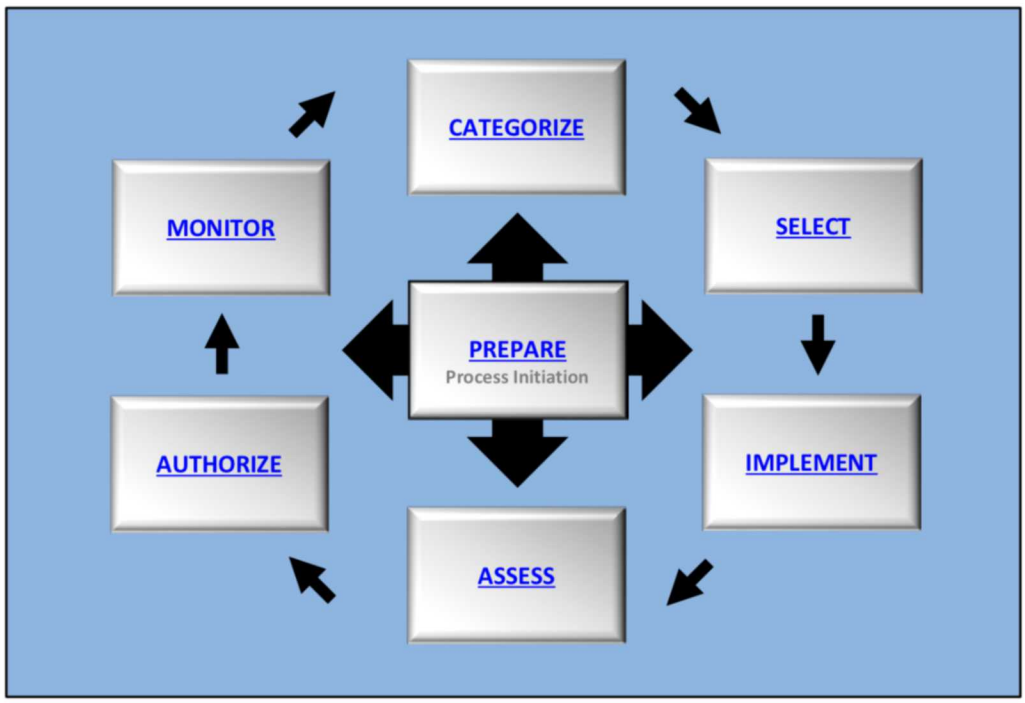


Figure 26. Risk Management Framework Tasks

Inter-organizational processes and roles and responsibilities add a valuable perspective. These differ from system environments of operations, and multiple interdependent environments of operations should be considered at the scale of an expanded paradigm. An example is Cloud hosted services where the data owner and data steward dichotomy rise to the level of separate systems and operations (On-Prem and Off-Prem). System cyber-relevant time is and should be faster than Process cyber-relevant time. It's important to note that flexibility is built into the NIST Risk Management Framework.

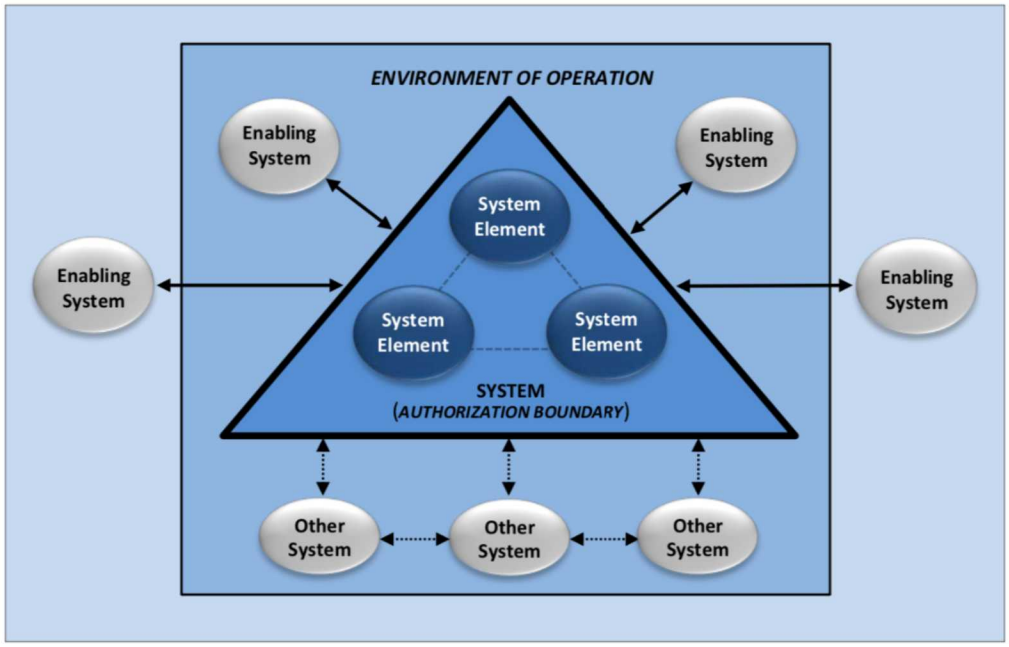


Figure 27. NIST RMF Conceptual View of a System and Environment of Operation

Separate data owner and data steward roles are considered in from a broader shared critical infrastructure perspective. In such case for this document, the On-Prem system is considered data-owner owned and controlled infrastructure, and conversely, the Off-Prem system is considered data-steward owned and controlled infrastructure.

The NIST Risk Management Framework offers the following definition of an Information Owner or Steward:

"INFORMATION OWNER OR STEWARD

The *information owner or steward* is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. In information-sharing environments, the information owner/steward is responsible for establishing the rules for appropriate use and protection of the information and retains that responsibility even when the information is shared with or provided to other organizations. The owner/steward of the information processed, stored, or transmitted by a system may or may not be the same individual as the system owner. An individual system may contain information from multiple information owners/stewards. Information owners/stewards provide input to system owners regarding the security and privacy requirements and controls for the systems where the information is processed, stored, or transmitted."

Further guidance may be found in the NIST Risk Management Framework document reference.

4.2. NIST Special Publication 800-160, Volume 2

The NIST Developing Cyber Resilient Systems: A Systems Security Engineering Approach, November 2019, calls out Cyber Resiliency as an increasingly necessary system property. The Systems Security Engineering approach is aligned with the system development life cycle through the recommended use of automated support tools. Cyber resiliency goals include: Anticipate, Withstand, Recover, and Adapt. Cyber resiliency objectives include: Prevent or Avoid, Prepare, Continue, and Constrain.

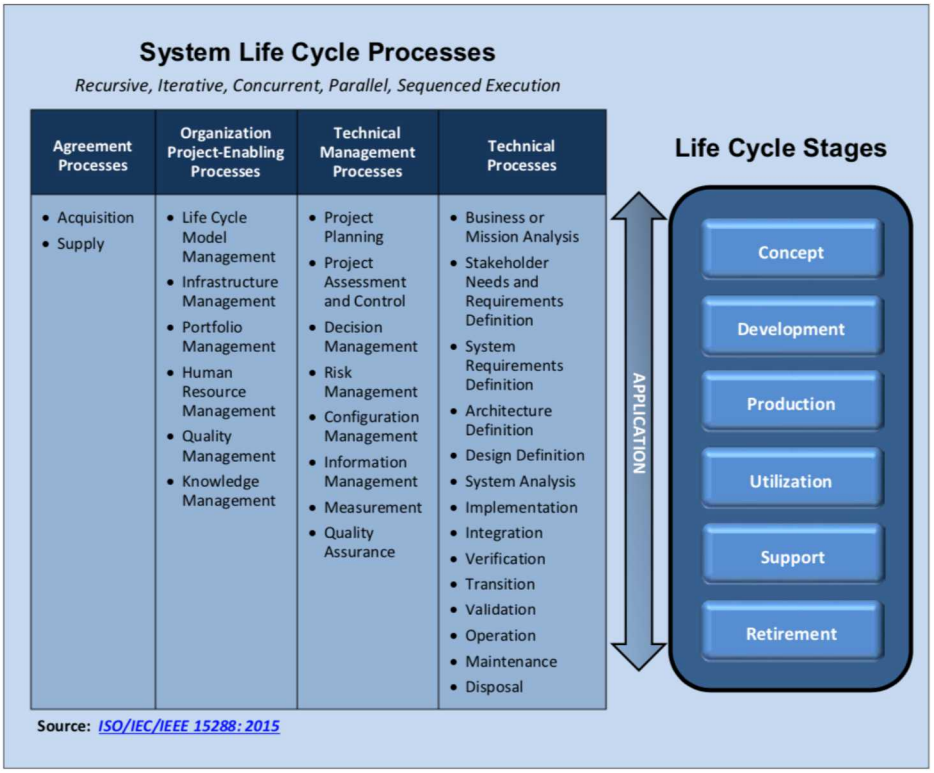


Figure 28. NIST SP800-160, v2 System Life Cycle Processes and Stages

Developing Cyber resilient goals and objectives may dovetail conveniently with the NIST CSF functions: Identify, Protect, Detect, Respond, and Recover. The use of multiple NIST guidelines is recommended for addressing the scale and interdependencies of the new digital technological paradigm.

This literature review finds that the NIST CSF, RMF, and the Developing Cyber Resilient Systems: A Systems Security Engineering Approach complement the increasing critical infrastructure protection demands of the changing cyber ecosystem.

NIST Developing Cyber Resilient Systems approaches are illustrated below.

Figure 29. Cyber Resiliency Techniques and Implementation Approaches

The CPR design approach uses preliminary risk and hazard assessments that then inform preemptive mitigations. Systems Security Engineering is useful in the development of security controls that instrument such preemptive mitigations. Conceptually, CPR design extends Cyber and system resiliency to include information resiliency through the data-centric information protection approach.

The process for defining Systems Security Engineering preemptive mitigations will vary to the specificity and protection requirements of each organization, system, and subsequent interdependencies. Similarly, but on a larger scale, CPR preemptive mitigations extend beyond a systems perspective to a critical infrastructure sector and sector interdependencies perspective relevant to the expanding and integrated OT/IT/IoT cyber ecosystem.

The NIST SP 800-160, v2 offers the following description of Critical Infrastructure Systems:

"**Critical Infrastructure Systems**

Critical infrastructure systems are often specialized, high-confidence, dedicated, purpose- built systems that have highly deterministic properties. As such, these systems often have limitations regarding storage and processing capabilities; strict timing constraints; and severe if not catastrophic consequences of failure. "

Furthermore, the DMTF and IEC CIM standards may be useful in definition of complex systems, system of systems, intersystem dependencies, and hierarchy. An IEC Energy CIM example is illustrated in the Energy Field Area Network Common Reference Architecture.

Further guidance may be found in the NIST Developing Cyber Resilient Systems: A Systems Security Engineering Approach document reference.

4.3. Data Centric Protection Approach

The enterprise perimeter has evaporated with the innovation of mobile and Cloud technologies. These technologies have changed nature of the communication and computing paradigm to a data everywhere, user anywhere model. Therefore, data-centric protection is necessary along with conventional system and network protection mechanisms.

An accompanying shift in infrastructure roles and responsibilities is inherent in the migration of information assets from an On-Prem data owner-owned and controlled infrastructure "enterprise perimeter" to a porous Off-Prem data-steward owned and controlled infrastructure. This expands information assurance to a multi-stakeholder security posture. For example, a CSP who shares in the responsibility of data protection and information assurance.

The CPR design approach includes a brainstorming session to assist in the development of data-centric protection.

Topics:

- Information Value and Residence
- Infrastructure Maturity / Modernization
- Data and Service Location
- Service Delivery
- Information Asset Security

Questions and Intent: Information Protection

- What challenges can be identified?
- What security architecture insights can be identified?
- What security risk/mitigation concerns can be identified?
- What priorities can be identified?
- What use cases / analytics can be identified?
- Path Forward:

Each area may be further articulated as follows:

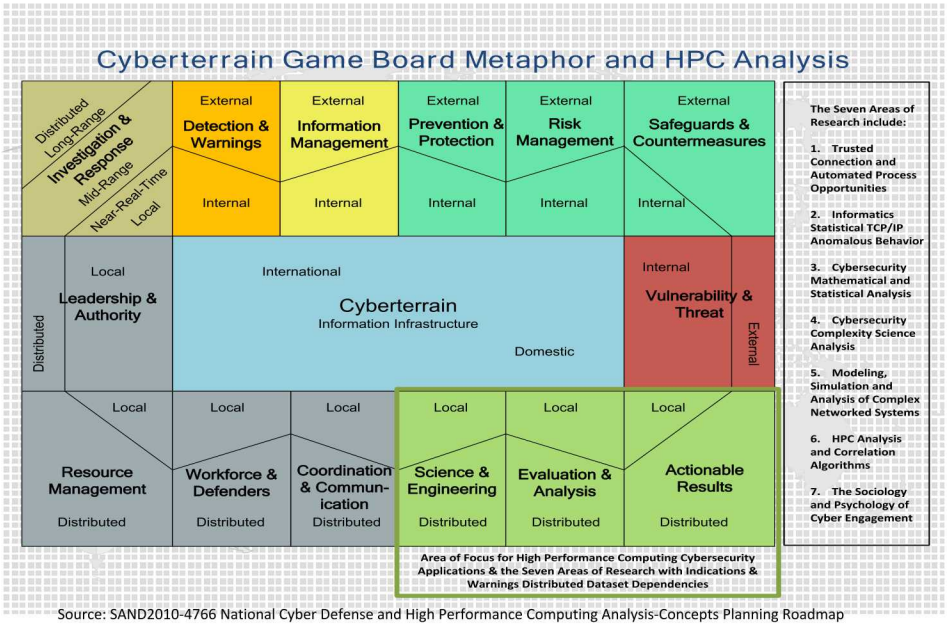
- Topic 1 - Information Value and Residence
    - Authorization – Designated Approving Authority, FEDRamp, Other
    - Public – Non-Sensitive Information
    - Private – Sensitive Information
    - Data Ownership – Agency, Organization, Community, Individual
    - Data Stewardship – 3rd Party, Provider
    - Elastic – Ephemeral, Short Lived, Instances
    - Records – Long Lived
    - Information Assurance – Authentication, Inheritance, Multitenant, Cyber Security Framework
- Topic 2 - Infrastructure Maturity / Modernization
    - Organization – Government, Agency, Department, Enterprise, Corporate, Business
    - Provider – CSP/ISP
    - Information Systems – Computing, Platform, Vendor, IT
    - Operational Systems – Life Safety, Physical Security, Facilities, OT
    - Operational Support Systems (OSS) – Domain Name Service (DNS) Address Records (A/AAAA), IP Address Management (IPAM), Incident Response, ICAM, Directory Services
    - Services – Legacy, Cloud, EaaS, SaaS, PaaS, IaaS
    - Network – IPv4, IPv6, Dual Stack, Wireline, Wireless 5G, Mobile, Broadband, Communications
- Topic 3 - Data and Service Location
    - Internal – On Prem, Private Cloud, Local
    - External – Off Prem CSP, External Facing Services (DNS, Email, Web), Distributed

- Internal/External – Dependencies, Caveats, Differences, Separation

- Topic 4 - Service Delivery
  - Physical – Hardware, Device, Client/Server, Wireline
  - Virtual – Cloud, Software Defined Radio (SDR), SDN, ML, AI, VR, AR
  - Mobile – Wireless, Mobile Networks, Near Field Communications, Intranet, Internet

- Topic 5 - Information Asset Security
  - CPR Design Principles – Confidentiality, Integrity, Availability
  - Confidentiality (C) – Encryption at Rest, In Transit, In Process
  - Integrity (I) – Validation, Authorization, Authentication, Audit
  - Availability (A) – Virtual, Multisource, Multipath, Mobility, Portability, Staffing, Skills Development
  - Data Protection – Identity, IT (CIA), OT (AIC), OSS
  - Information Processing – Control Plane, Management Plane, Data Plane
  - Vulnerability – Risks, Change, Configuration, Partners, Processes, Operations, Technical, Administrative
  - Threat Exposure – Services, Neighborhood, Organization, Mobile, Device, Supply Chain, User, Insider
  - Resilience – Critical Infrastructure, Remote Operations, Resource Diversity, AppSec

The Data Centric brainstorming session should involve multistakeholder participation. A "Cyber Peanut" gameboard metaphor was developed for a 2010 Cyber Defense and High Performance Computing Analysis – Concepts and Planning Roadmap. The gameboard is a useful tool to frame participant roles and responsibilities for the brainstorming session.



Source: SAND2010-4766 National Cyber Defense and High Performance Computing Analysis-Concepts Planning Roadmap

Figure 30. Cyber Peanut Game Board - Functions, Roles, and Responsibilities

The Data Centric brainstorming session goals are to define unforeseen challenges, insights, and opportunities as organizations wrestle with technical investments and security requirements in the changing cyber ecosystem. An example brainstorming results table is illustrated below:

Information Protection & Insights	Information Value & Residence	Infrastructure Maturity/ Modernization	Data & Service Location	Service Delivery	Information Asset Security
Challenges Identified	On-Prem Data Owner to Off-Prem Data Steward Control	STEM Next Gen, Identity Credential & Access Management	On-Prem / Off-Prem Workload Transition	Physical, Virtual, Mobile Presence	Tactical / Strategic Data Centric Protection
Security Architecture Insights	Data and User Residence & Location (Virtual & Mobile); Data Everywhere; User Anywhere	Legacy vs. Current Standards & Dependencies, Preemptive CPR Design	Cloud / Virtual / Mobile Dependencies; Internal / External Protections, Multi-Org Identity Credential & Access Management	Multi-Stakeholder Cyber Relevant Time; CSF Functions	OT-IT Integration; In-Process; In-Transit; At Rest; Operational Support Systems (OSS)
Security Risk / Mitigations	Authorization, Access Control, & Trust	Buyer / Supplier Incident Response, Collaboration	Preemptive CPR Design, NIST Cyber Security Framework (CSF), OT-IT AIC^{2}IA	Data Centric; End Point Security	Consistent OT-IT, On-Prem / Off-Prem/Mobile Data Protection
Priorities	Information Assurance	Workforce Dev, ICS / SCADA Protection	Data Centric Protection	Timely / Secure Delivery	Baked-In Security; Ongoing Diligence
Use Cases / Analytics	Virtual Connectivity / Anomalistic Analytics	Critical Infrastructure Protection at Scale / ICS-SCADA Statistical Analytics	Changing Cyber Ecosystem / OT-IT-Comms-Systems Analytics	Stakeholder Roles / Behavioral Analytics	Cyber Disruption Response & Recovery / Indictor Analytics
Path Forward	Data Centric Assurance	Divest Old / Invest in New Standards, Train	Secure / Design / Build Scalable Technologies	Secure Deploy New Services	Scalable Standards-Based Security

Table 6. Data Centric Brainstorming Example Results

4.4. Cyber Risk Assessments

Cyber design comprises enterprise and buyer/supplier service providers. This is both an internal and external view of information value and protection. Cyber risk assessments may take several approaches depending on the scale of the system or system of systems, value of information and infrastructure assets, and severity of security events. A few of these are discussed herein.

4.4.1. Administrative Risk

Policies for organizational guidance inform the workforce as the first line of defense. Practices and processes similarly impact administrative risk, which can be viewed as day-to-day activities. In this case redundancy, routine, and complacency can exacerbate administrative risks.

4.4.2. Technical Risk

Technical investments past, current, and future impact the scope of technical risk. Technical cover technologies comprised in the deployment of existing operations. The risk of new technologies is to be conducted against this operational posture. For example, IPv4/IPv6, 4G LTE/5G NR – WiFi6. Mitigations include high-availability and response to compromise of IT and Communications critical infrastructures.

4.4.3. Operational Risk

Operational Security (OPSEC) and operational technology security impact the scope of operational risk. New technology deployments impact operational risk in terms of workforce readiness, incident response and overall visibility into situational awareness of the organizations operating environment.

4.4.4. Physical Risk

Physical security systems are network and computing dependent. Examples include IP connected cameras and motion detectors. Access control systems to grounds and facilities are similarly dependent for alarm and notification systems for protective force response. These type of safety and security systems are good examples of OT/IT/IoT integration.

Physical security systems commonly run over the same network as IT. There are security requirements differences in IT versus OT systems. Furthermore, OT systems such as safety and security systems are part of the so called IoT. IT and OT devices, such as cameras, are now part of the "systems" instrumentation occurring as part of vast broadband and device connectivity potential in unserved and underserved areas. Mitigations include perimeter, access control, and response to intrusion of critical infrastructures.

4.5. Design Assessments

Design assessments may be used with new "baked-in" security purpose, whereby preliminary assessments inform a higher starting security posture for CIP. Information elicited from such preliminary or front-end security assessments will be used to implement critical infrastructure preemptive mitigations. It should be noted that this is an out of the gate improvement only, and ongoing critical infrastructure security posture diligence is necessary to develop mitigations in an ongoing and evolving technological basis and associated evolving threat exposures.

4.5.1. Physical Risk Assessments

Physical security systems are network and computing dependent. Examples include IP (IPv4 and IPv6) connected devices such as cameras and motion detectors. Access control systems to grounds and facilities are similarly dependent for alarm and notification systems for protective force response. Such systems may be considered as OT.

Source: https://cloud.google.com

4.5.2. Hazard Assessments

Hazard assessment for natural disasters set the preparedness level for seldom occurring events that may be the most wide spread and disruptive to business operations. Business continuity and continuity of operations planning are

important to establish preparedness for such events. Key concerns are first and foremost life safety. Emergency management addresses the protection of people, property, and the environment. Precedence is given to emergency management to ensure that the environment and facilities are safe before cyber disruption response and recovery activities begin and are completed to resume normal operations. Important areas to consider are vital records, critical functions, and essential personnel.

4.5.2.1. Natural Hazards

This will include impact assessment of natural hazards such as flood, fire, and weather-related disruptive events. This also includes pandemic preparedness and response. Precedence is given to emergency management to ensure that the environment and facilities are safe before cyber disruption response and recovery activities begin and are completed to resume normal operations. Important areas to consider are vital records, critical functions, and essential personnel.

4.5.2.2. Manmade Hazards

Hazard assessment for manmade disasters set the preparedness level for seldom occurring events that may severely disrupt business operations. Business continuity and continuity of operations planning are important to establish preparedness for such events. Key concerns are first and foremost life safety. This will include impact assessment of manmade hazards such as terrorist or cyber-attack and related disruptive risks. Similarly, precedence is given to emergency management to ensure that the environment and facilities are safe before cyber disruption response and recovery activities begin and are completed to resume normal operations. Important areas to consider are vital records, critical functions, and essential personnel.

4.5.2.3. Technological Hazards

This will include impact assessment of technological hazards such as telecommunications outages, power outages, water shortages and related disruptive events. Supply-chain disruption may also factor into readiness and continuity of operations with impact to safely respond and recover to normal operations. Important areas to consider are vital records, critical functions, and essential personnel.

4.6. Operational Security

Operational security (OPSEC) is often used with the phrase “See Something, Say Something” intended to enlist a workforce culture of caution. The first line of OPSEC defense is a trained, knowledgeable, and aware workforce.

The Department of Energy Handbook for OPSEC, DOE-HDBK-1233-2019 June 2019 refers to OPSEC as a five-step process. The five steps of the OPSEC process are:

Step 1 – Identification of Critical Information
Step 2 – Analysis of Threats
Step 3 – Analysis of Vulnerabilities
Step 4 – Assessment of Risks
Step 5 – Application of Appropriate Countermeasures

DOE-HDBK-1233-2019 further states that:

“**Internet**
One of the greatest indicators of DOE programs, practices, intentions, and procedures is the internet. The proliferation of use for email, social media, marketing, and other information exchanges is explosive. The highly vulnerable internet has become a vast treasure chest of free information for commercial, political, and military adversaries of the United States, activists, terrorists, and criminals. The threat to information placed on the internet is stated repeatedly and constantly in both the commercial and government arenas. Hardly a day goes by when newspapers or other news media do not have a story about some great hacker success, or some theft or fraud committed by individuals abusing the internet.

Radio and Telecommunications

Radio and telecommunications may be assessed based on inherent vulnerability to monitoring. Many DOE facilities depend heavily on radio communications and virtually all facilities depend on telecommunications. Vast amounts of data and information are exchanged on these systems. In an effort to understand what equipment is used at the site, where it is located, how it is used, and known vulnerabilities, the OA team should attempt to diagram the system in cooperation with the chief information office. The OA should, in cooperation with the Chief Information Office, identify the equipment in use; assess susceptibility to intercept; and identify particularly vulnerable nodes. Radio communications may range from a few handheld units to multiple nets with repeaters covering hundreds of square miles and uniting outlying sites. The first step in data collection for radio communications is to obtain a comprehensive listing of the nets and their frequencies showing:

Users

- Sensitivity of traffic
- Types of equipment employed
- Function
- Periods of operation
- Use of repeaters
- Power levels
- Any unique features (e.g., telephone patch) "

Figure 31. Radio and Telecommunications Diagram, DOE-HDBK-1233-2019

Internet and radio and telecommunication dependencies similarly impact tribal, local, and state facilities. Three levels of rigor are also discussed: Sufficient, Rigorous, and Restrictive depending that criticality, sensitivity, and value of information.

Internet Engineering Task Force (IETF), informational Internet draft addresses Operational Security Considerations for IPv6 Networks. It states:

"Knowledge and experience on how to operate IPv4 securely is available: whether it is the Internet or an enterprise internal network. However, IPv6 presents some new security challenges. RFC 4942 describes the security issues in the protocol but network managers also need a more practical, operations-minded document to enumerate advantages and/or disadvantages of certain choices.

This document analyzes the OPSEC issues in several places of a network (enterprises, service providers and residential users) and proposes technical and procedural mitigations techniques."

4.7. Cyber Physical Resilient Design

Preemptive risk and hazard assessments inform design parameters as an advantage for a more secure posture for the three elements of risk concern (cybersecurity, physical security, and resilient design requirements). Taken as a set of preemptive security design measures they collectively elevate the protection posture of an organization.

CPR design practices are a starting point with preemptive assessments and analysis for new build technologies, new services areas, and new service development. A designed in protection posture elevates the organization, although continual oversight is required to quickly respond and recover from cyber disruptive events. The NIST CSF: Identify, Protect, Detect, Respond, and Recover functions provide a framework for CPR design.

4.8. NIST Cyber Security Framework

Cybersecurity actions is comprised of essential controls that are illustrated as part of The CSF functions, which further provide guidance to manage cyber events. The adoption of cloud services expands information management and protection from within an organization to an inter-organizational and interconnected information and communication protection posture.

The NIST CSF is a voluntary set of standards and best practices intended to help organizations across the public and private sectors manage cybersecurity risks. The CSF conceptualizes five functions in the cybersecurity risk management process, outlined in below.[6]

Function	Definition	Categories
Identify (ID)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
		Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
		Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
		Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
		Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
		Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with

[6] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Function	Definition	Categories
		managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.
Protect (PR)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	**Identity Management and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.
		Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
		Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
		Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
		Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
		Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Detect (DE)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
		Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
		Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
Respond (RS)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
		Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
		Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
		Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
		Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and

Function	Definition	Categories
		previous detection/response activities.
Recover (RC)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
		Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
		Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Table 7. Overview of NIST CSF Functions

5. RESPONSE AND RECOVERY FROM CYBER DISRUPTIVE EVENTS

The early days of the Internet facilitated friendly intercommunications. Security was most often not an issue or design requirement. Circa 1993 the world-wide web was born, and subsequently untrusted intercommunications became common place. Such untrusted communications exposed the vulnerabilities of complex network and computing technologies. Cybersecurity design was and is all too often an afterthought from vendors with priority set on profitability and getting products fast-tracked to market to beat the competition. The industry has since been trying to catch up, which has resulted in bolt-on security, after the fact, resulting in scrambling to rollout patches to shore up cybersecurity. This is unacceptable for critical infrastructure.

Specific threats of the day span a wide variety of threat-vectors, threat-actors, and risks to critical infrastructure information assets. Automated threats such as botnets and ransomware attacks are affecting organizations worldwide.

ICAM has become a source of core indicators of compromise, which can provide timely identification and visibility to an organization and business partners, including services providers and supply chain.

5.1. Identity Credential and Access Management

Identity, Credential, and Access management, or ICAM enforce authorized use and authentication for access to information systems and information assets. ICAM is also referred to Identity and Access Management, or IAM. ICAM may be applied to information systems within an enterprise network with well-defined perimeters with common tool suites such as the lightweight directory access protocol (LDAP), which may serve as an authoritative source for identity information. New ICAM challenges arise when information assets are outside of well-defined enterprise network perimeters, such as Cloud services hosted by CSP's. ICAM Authority and methodologies can become very complex in the Data Everywhere-User Anywhere paradigm. The disciplines of identity management, credential management, and access management for ICAM are discussed below.

5.1.1. Identity Management

Identity management is the effective control of providing access for authorized users of information and communication technology (ICT) to information assets. Processes include on-boarding new users, managing access throughout the lifecycle of information, and off-boarding users who no longer require access to information.

5.1.2. Credential Management

Credential management is the effective control of credentials assigned to individual users to verify and validate authorized access to information assets. Public Key Infrastructure (PKI) and LDAP are common means of managing identity and credentials for a user's daily access to information assets.

5.1.3. Access Management

Access management is the effective control of authorized access to information assets. Processes span the functions of human resources, business, organizational, buyer and supplier, and ICT implementation of controls to assure access to information assets. Likewise, the removal of access when it is no longer required is as fundamental as authorized access itself.

5.2. Cloud Security Practices

This review does not recommend any vendor or product over another and is intended as an objective advisory. Given that CSPs are continually updating their service offerings, this review represents a fall 2019 "snapshot in time" of available data protection and security practices.

5.2.1. Least Privilege

Least privilege is the principle of assigning user accounts or processes the rights and privileges that are essential to the roles and responsibilities of that job. Critical examples of implementing least privilege in Cloud ICAM are:

- Avoid primitive and overarching roles that are native to CSPs and invite most users to be categorized in roles that do not fit their job description.
- Create a separate service account for each of the services, with appropriate permissions granted to each service account
- Grant roles the smallest permissions possible
- Restrict user accounts that can act as service accounts
- Restrict the number of users who can create service accounts
- Ensure parent permissions do not conflict with child permissions

5.2.2. Service Accounts

Service accounts are user accounts that are used for automated processes that need permissions to access resources on the cloud. Service accounts use keys instead of passwords. Managing these services is critical to security, some examples of implementing this security are:

- Rotate service account keys.
- Implement automated processes to manage service accounts and their keys.
- Ensure that service accounts are not deleted prior to those services being shut down.
- Don't upload service account keys to the CSP.

5.2.3. Auditing

It is important for agencies to audit the risk that having agency data and resources in the cloud. It is important to have policies in place to ensure auditing is done:

- Alert on any changes to the organization's Cloud ICAM policy to ensure the changes were appropriate and are reviewed on a regular basis.
- Export logs to a storage location to ensure they are not deleted and there is no information loss.
- Check which users can change ICAM policies
- Check access to: logs, service account keys, etc.

5.2.4. Policy Management

Access to cloud computing resources is controlled by creating policies and assigning those policies to users, groups or roles.

- Set policies for all projects in the organization
- Grant roles to groups instead of users

5.2.5. Centralize Identity Management

Integrate on-premises and cloud ICAM directories to ensure that all identity data is stored in one location.

- Consistency and a single authoritative source will increase clarity and reduce security risks from human errors and configuration complexity.
- Don't synchronize accounts to cloud identity stores that have high privileges in your existing Active Directory instance.
- Turn on password hash synchronization.

5.2.6. Connected Tenants

In the cloud an organization will likely have multiple tenancies in each cloud. It is important that the organization's security organization has visibility into all subscriptions that are connected to the on-premises environment.

5.2.7. Single Sign-On

Single sign-on services enable users to access cloud services and applications from multiple devices without the need to repeatedly enter credentials. Organizations can enable automatic access provision to users based on employment status.

5.2.8. Conditional Access

User identity is not the only compliance that an organization may want to enforce. Determining not only who can access a resource, but from where and which device is important as well. Conditional Access can help make automated decisions based on access control policies.

- Manage and control access to an organization's resources based upon group, location, application sensitivity, etc.
- Block legacy authentication protocols from having access to all relevant applications.

5.2.9. Password Management

Ensure that password management protections are in place to protect the organization against users abusing security policies.

- If it aligns with organizational policy enabled password resets to be performed by the users.
- Log and investigate how password reset is being used.
- Ensure password policy is consistent on the cloud and on-premises by updating policies at the same time, including banned password lists, etc.

5.2.10. Multi-factor Authentication

Multifactor authentication (MFA) combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

5.2.11. Role-Based Access Control

Designating groups or individual roles responsible for specific functions in the cloud helps avoid confusion that can lead to human and automation errors that create security risks. Restricting access based on the need to know and least privilege security principles is imperative for organizations that want to enforce security policies for data access.

- Separate duties and have clear roles for users where possible to allow access to those users that they need to perform their job.
- Ensure security teams have access to the RBAC to periodically review and remediate risks
- Use built-in roles where appropriate, but create new custom roles if no built-in role fits that user's role

5.2.12. Privileged Accounts

Privileged accounts are the most sought-after accounts by attackers. Organizations want to ensure that the minimum number of privileged accounts exist, that the minimum number of users have access to those accounts, and that all privileged accounts have all necessary protections.

- Manage, control, and monitor access to privileged accounts.
- Ensure that admin accounts are managed by the CSP and not a personal user account
- Ensure admins have separate accounts for each role they perform
- Identify and categorize accounts that are in highly privileged roles. In addition, closely monitor those accounts and any activity on those accounts

- Ensure that privileged accounts take advantage of temporal roles to limit exposure
- Assign emergency accounts to your organization
- Restrict access on privileged accounts (i.e. limit web-browsing and email attack vectors)
- Deprovision accounts when accounts are no longer in use
- Regularly test accounts using cloud testing environments to test current attack techniques
- Ensure separate user accounts and mail forwarding for global administrator accounts
- Have an appropriate password policy that requires frequent password changes
- Use cloud-based risk assessment tools to assess policies and the state of identity stores

5.2.13. Monitoring

An active identity monitoring system can quickly detect suspicious behavior and trigger an alert for further investigation.

- Identify sign-in attempts
- Determine brute force attacks against a particular agency account
- Find login attempts from multiple locations at similar times or from a suspicious location
- Logins from infected devices
- Use threat feeds to determine suspicious login attempts by IP address
- Review CSP reports on anomalous activities
- Use CSP risk monitoring system to evaluate risk based upon agency need

5.2.14. Identity Stores

When moving to the cloud ensure that on-premises identity repositories can be extended to the cloud. Most organizations use a popular repository such as Active Directory, which most CSP will support. However, custom identity types will have to be evaluated to see how they interact with a particular CSP.

5.2.15. Federation Capabilities

According to IETF Request for Comment (RFC) 7832, Application Bridging for Federated Access Beyond the Web (ABFAB) Use Cases, May 2016: “Federated identity facilitates the controlled sharing of information about people (a.k.a. "principals"), commonly across organizational boundaries. This avoids redundant registration of principals who operate in and across multiple domains, both reducing the administrative overhead for the organizations involved and improving the usability of systems for the principal.”

5.2.16. Password Policy

Credential strength is directly related to length, reuse, complexity, randomness, and storage. Cloud providers may or may not offer technical enforcement of organizational password policy. This can require further user training and administrative controls to ensure alignment with organizational cybersecurity requirements.

5.2.17. Temporal Roles

Cloud services permit on-demand granting of privileges or access. On-demand access can be granted for both programmatic and user interaction with services and systems. This further enables tenant organizations to implement least privilege and reduce the frequency of credential passing where it may be subject to interception, observation, hijacking, or modification.

5.3. ICAM in the Cloud

The data captured by various vendors within a given cloud-service type are generally similar: Typically, the data fields offered by competing vendors within a given service type are comparable. In other words, literature review found few instances of one vendor offering a type of data that its competitor(s) did not.

The data offered by various vendors provide insufficient coverage for full protections: CSP offerings do not natively support full data-protection requirements and must utilize complementary services to achieve desired results. Moving data to the cloud necessarily changes the strategies needed for protecting that data. Consequently, existing tools and approaches must be enhanced to perform under this new model.

5.3.1. User Management

User management is the combination of technical systems, policies, and processes that create, define, govern, and synchronize the ownership, utilization, and safeguarding of identity information. The primary goal of identity management is to establish a trustworthy process for assigning attributes to a digital identity and to connect that identity to an individual. Identity management includes the processes for maintaining and protecting the identity data of an individual over its life cycle.

The user lifecycle begins when a user account is granted access to information systems. The lifecycle continues throughout the authorized use of information and network resources. Information assets, whether physical or virtual, comprise the creation, processing, transportation, and storage of information. Information value assessment drives the protection posture necessary for sufficient confidentiality, integrity, and availability of information. The composite entitlements and access to information are a product of accumulated entitlements that vary depending on the duties that a particular user may have to perform. A user may at different times perform privileged and sensitive operations such as configuration management or identity management authorization. Separation of duties, least privilege, auditing, and accountability all factor into the lifecycle management of an "identity, or electronic entity that represents a user of information systems.

5.3.2. Authentication Management

Determines who an entity is, based on one or multiple factors: something the user knows such as a password or pin; something the user has such as a personal identity verification (PIV) card; something the user is such as a fingerprint. The strength of these factors and their required complexity is balanced against the sensitivity of the protected data.

5.3.3. Authorization Management

Determines rights and privileges an entity has based on policies and roles. Authorization management may consider time-of-day, device type, location such as mobility, and role that an entity (user or service) exercises as comprised by organizationally definition of authorized duties.

5.3.4. Access Management

Access control policies that enforce entity access to Cloud resources. Access management may consider data sensitivity, type-of-service, lifecycle, time-of-day, device type, location such as mobility, and role that an entity (user or service) fulfills in the performance of authorized access and responsibilities.

5.3.5. Data Management

A set of processes and tools that provision identities and data within authorized guidelines. Authorized data management guidelines may include day-to-day activities of an authorized entity (user or service account) that are aligned with data sensitivity, type-of-service, and lifecycle. Day-to-day activities should be independently managed and performed from privileged activities of an authorized entity.

5.3.6. Monitoring and Auditing

Authorization, audit and accountability, and monitoring provide a measure of verification and validation for appropriate data accesses within authorized activities. Such measure may reveal indicators of compromise and increased visibility and situational awareness of operational deficiencies.

5.3.7. Application Program Interfaces

Application program interfaces (APIs), defined as "a set of subroutine definitions, protocols, and tools for building application software."[7] Organizations moving to cloud environments can leverage commercially provided APIs, open source APIs, and develop custom APIs.

5.4. Cyber Relevant Time

CRT is a relative value based on the attack speed of the adversary and the response time of the network defender. Additionally, large organizations that leverage complex technologies ultimately share roles and responsibilities for network defense. Organizations and vendors share roles and responsibilities for oversight and resolution of cybersecurity events. This relationship between organizations and vendors expands in the context of cloud computing with additional challenges requiring unique guidance to detect and respond to cyber events effectively.

An elevated protection posture gives the defender an advantage in an attacker/defender set of actions. An attacker/defender timeline is illustrated below.

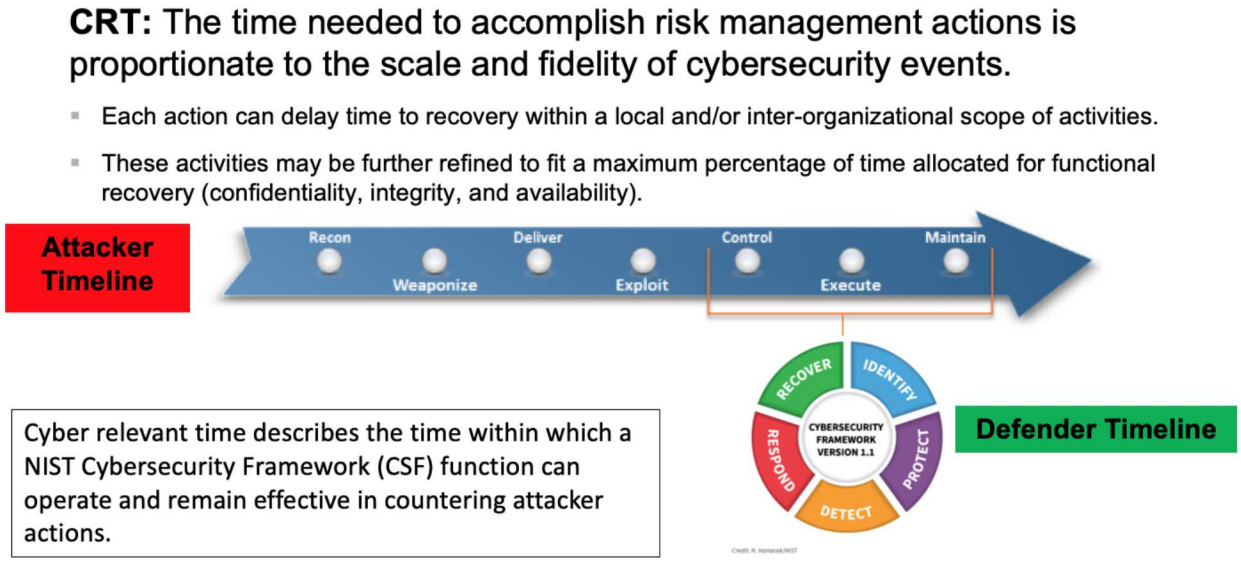


Figure 32. Attacker vs. Defender Timeline

Other cybersecurity tool suites may be considered in a holistic organization/vendor protection approach. For example, an organization protection posture may include monitored Internet connections and intrusion protection/prevention tool suites. These tools rely on different but related datasets that may be useful in an expanded CRT definition.

[7] https://en.wikipedia.org/wiki/Application_programming_interface

The table below illustrates an example of potential alignment of cybersecurity tools with buyers and suppliers.

Cybersecurity Functions	Buyer	Supplier
On-Prem Tools:	Organization	Commercial
Risk Management/Awareness	Organization	Commercial
Managed Asset/Access ISP Network Monitoring	Organization	Commercial/ Internet Service Provider (ISP)
Intrusion Protection/Prevention	Organization	Commercial
Off-Prem Tools:	Organization	Cloud Service Provider (CSP)
Shared Tenant Cloud Service Shared Risk Management/Awareness	Organization	Commercial/CSP
Shared Distributed Asset/Access	Organization	Commercial/CSP
Shared Network Monitoring	Organization	Commercial/ISP/CSP
Shared Intrusion Protection/Prevention	Organization	Commercial/CSP

Table 8. Cyber Relevant Time: Buyer/Supplier Roles and Cybersecurity Functions

The changing cyber eco-system is broad and complex. CSF alignment permits an opportunity to frame the problem into a manageable and comprehensive CPR perspective. Cyber response and recovery are relative to the scale and scope of an incident. The various technologies also must be understood and well-managed for effective response and recovery to disruptive cyber events.

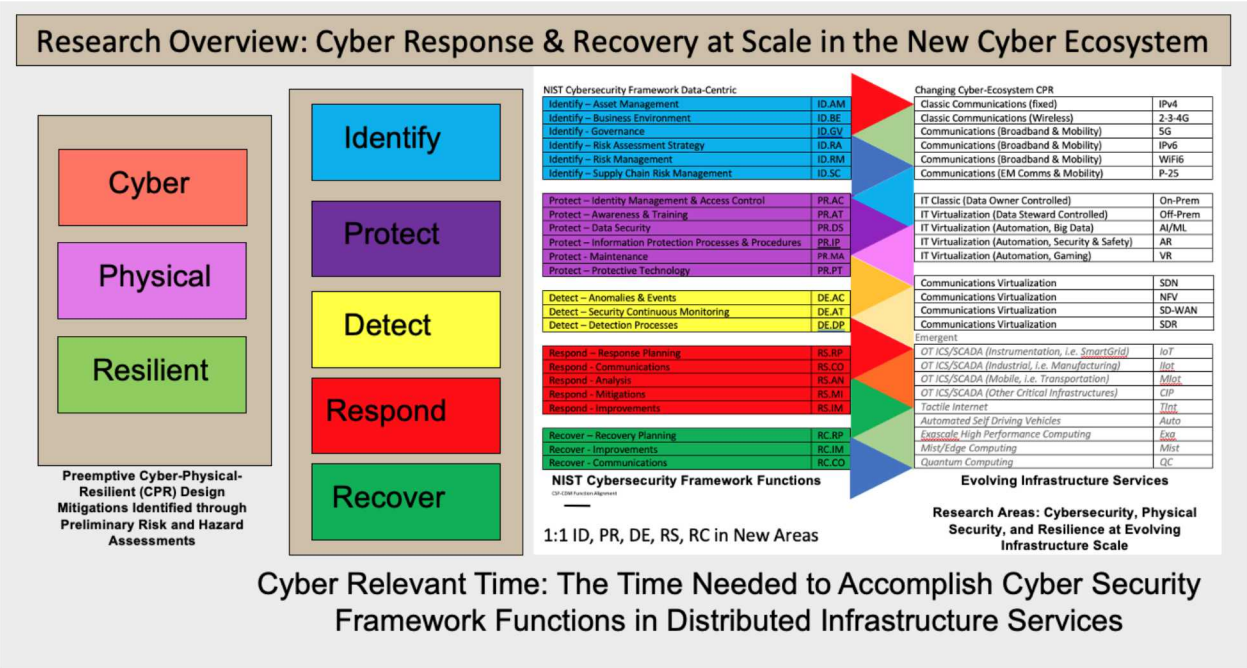


Figure 33. CPR-CSF Mapping to the Changing Cyber-Ecosystem

5.5. Cybersecurity

Cybersecurity comprises all automated information processing strata. IT, OT, and IoT are foundational concerns. Various and differing inter-organizational automated information processing paradigms may complicate the complexity and veracity of cybersecurity. Examples include: Cloud services; mobility; and the digital dichotomy. Users may need to have access to multiple modalities of computing and communications to meet their responsibilities.

Enterprise data centers still provide IT and OSS services, such as DNS, IPAM, SOC/NOC functions, and hardware and software inventories. In contrast, virtual infrastructure and mobility change the paradigm completely, including emulated services that can obfuscate authoritative identity repositories. The core CSF functions and ICAM become very difficult to ascertain in multi-stakeholder distributed system, device, and user deployments.

5.5.1. Operational Support Systems

OSS comprise the behind the scenes services that make IT work, and the back-office financials and "middleware" that perform automated job processing in the middle of the night. OSS functions will expand as OT becomes more compute and network centric; and as virtualized service adoption expands to host evermore data-owner information in data-steward owned and operated infrastructure. OSS systems include fundamental services such as the DNS, network time synchronization with Network Time Protocol (NTP) and multiple time sources, ICAM, and IPAM.

5.6. Adoption of the NIST Cyber Security Framework

The NIST Framework for Improving Critical Infrastructure Cybersecurity[8] is widely accepted at the national scale. It provides a core set of functions that fundamentally describe cybersecurity actions.

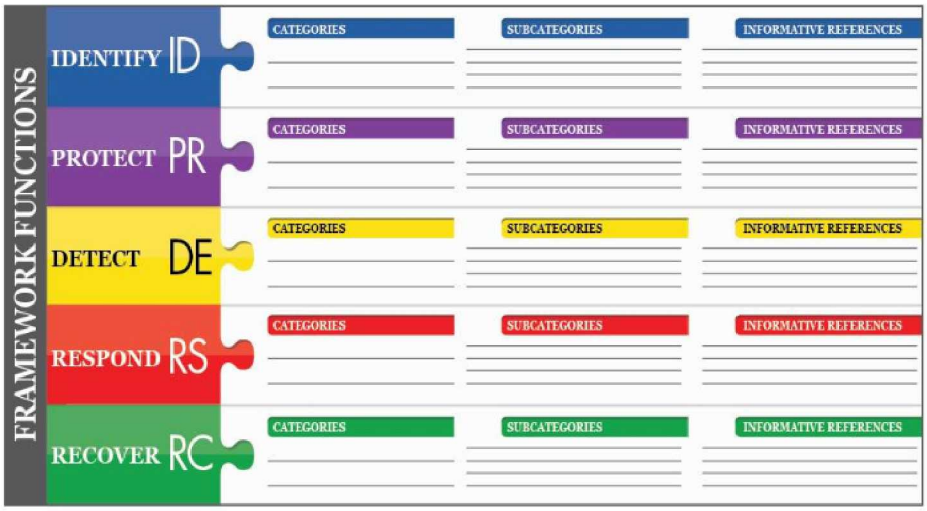


Figure 34. NIST CSF Core Structure

5.6.1. Implementation Tiers

The CSF implementation Tiers provide a view of maturity of organizational infrastructure readiness in terms of cybersecurity risk and how cybersecurity risk is managed. Para-phrased descriptions are included below.

5.6.1.1. Tier 1: Partial

Risk Management processes are not formalized leading to ad hoc and reactive response to intrusion. Integrated risk management programs are fragmented resulting in limited awareness at an organizational level. External participation is limited to a local perspective without participation in the larger cyber-ecosystem.

5.6.1.2. Tier 2: Risk Informed

Risk Management processes are formalized, approved by management and informed by organizational risk objectives, threats, and business requirements. Policy development and enforcement may not be consistent at a larger organizational level. Integrated risk management has increased awareness at the organizational level, although programs may not be established or consistent at an organizational level. External participation is limited in the larger cyber-ecosystem and information is not consistently gathered or shared.

---

[8] April 16, 2018 Cybersecurity Framework Version 1.1. This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.041620188

5.6.1.3. Tier 3: Repeatable

Risk Management processes are formalized, approved by management and expressed as policy; risk management involves continuous improvement. Integrated risk management programs are established and consistent at an organizational level; workforce knowledge, skills, and abilities are current. External participation permits larger cyber-ecosystem contributions and information is consistently gathered and shared.

5.6.1.4. Tier 4: Adaptive

Risk Management processes are adaptive to changing risk and threat levels and use risk informed policies; risk management practices are informed and proactive. Integrated risk management programs are established and consistent with overall business risk management such as financial; workforce knowledge, skills, and abilities are part of an established cybersecurity culture. External participation is part of continuous monitoring, diagnostics, analysis, and mitigation; formal buyer/supplier agreements are in place to manage supply chain risk.

5.6.2. Cloud CRT and CSF Adaptation

CRT involves the time to accomplish CSF functions. Organizational and inter-organizational cyber-relevant times to accomplish the CSF functions are discussed below. A CSP is used as a framing reference for this discussion as it provides an example of buyer/supplier inter-organizational dependencies with impact to the timely resolution of cybersecurity functions.

CRT can be considered as a binding of buyer/supplier cybersecurity event resolution at the intersection of the CPR designed in security and the NIST CSF functions. The buyer/supplier relationship addresses a larger context with expanded roles and responsibilities for inter-organizational validation and resolution of cybersecurity events. The buyer/supplier relationship is important in the case of a variety of technical service providers, including CSP and ISP services. Note that inter-organizational response will be further exacerbated by interdependent system reporting cycle times.

Technical considerations include: CDM, IPAM, and ICAM. Other cybersecurity tool suites may be considered in a holistic buyer/supplier protection approach. For example, an organizations protection posture may include intrusion detection, prevention and data loss prevention tool suites. These tools rely on different but related data-sets that may be used in an expanded information model as development evolves.

The security impact of Off-Prem Cloud service adoption is two-fold: 1) Information, and therefore protection of information assets shifts to an expanded data steward role with responsibilities that impact the timeliness of cybersecurity event resolution; 2) System accountability and reporting shifts to a wide area interdependent set of functions that impact the timeliness of cybersecurity event resolution. The consequence of these impacts constitutes new dependencies or bindings that have not been exercised in conventional data-center services. Hence, a fresh set of advisories are necessary to protect information for much broader buyer/supplier cybersecurity event resolution. This priority is addressed in DHS CDM and Cloud protection services. Subsequently, the CSF becomes a National-Tribal priority alignment with the common goal of securing information at rest, in process, and in transit. These impacts, consequences, and priorities are the foundation for CRT/CSF security event resolution.

CRT is a broad concept that describes the amount of time in which a NIST CSF function can operate. CRT crosses buyer/supplier organizational boundaries, including system reporting cycle times. DHS guidelines currently recommend a reporting tolerance of 72-hours to the larger community. The 72-hour time tolerance may be considered as an inter-organizational baseline or ceiling from which organizations can work to establish thresholds of tolerance for various service disruptions. CSP/ISP and the On-Prem organizations SOC/NOC local cybersecurity event reporting can fall within a tolerance of 24-hours, which is within the 72-hour timeframe. The 24-hour time tolerance may be considered as a local baseline or floor from which organizations can work to establish thresholds of tolerance for various service disruptions. Service disruption tolerance is an important consideration for setting recovery goals from cyber-disruptive events to meet business specific requirements and operational efficiencies.

Dependencies are levied on CSP and ISP reporting capabilities and tools that may be subject to change over time. Subsequently, cybersecurity event reporting and resolution will depend on the best effort of service providers and the veracity of their capabilities and tools. Additional dependencies include latency of information (availability) of a variety of data-types within expected tolerances. It is important to identify and prioritize types of data for

information assurance. For example, access control transaction notifications which may need to be tracked in near real-time, while others can be hours in delay.

The Identify and Detect CSF functions most closely align with the 24-hour time tolerance. Sufficient notification may require service provider service level agreements (SLA). The Protect, Respond, and Recover functional timeframes are considered greatly variable as these may depend on more involved inter-organizational interactions, capabilities, tools, and the level of effort driven by the scope and scale of risk and/or intrusion.

Cyber events vary in the scale and fidelity needed to accomplish risk management actions. Each action can delay time to recovery within a local and/or inter-organizational scope of activities. These activities may be further refined to fit a maximum percentage of time allocated for disruptive event tolerance and effective functional recovery (confidentiality, integrity, and availability) of an information asset or set of assets. Organization specific time-to-recover tolerances can be based on the criticality of services, applications, systems and data. MTTD and MTTR[2] metrics may inform and improve CRT tolerances.

Future development may include an expanded scope of virtual services, for example AI, ML, AR and VR, and software defined infrastructure services, such as SDN and SDR. These implicate other types of evolving service provider functions. Further alignment consideration could be given to the NIST RMF[9] for Information Systems and Organizations, SP 800-37, revision 2: Prepare; Categorize; Select; Implement; Assess; Authorize; and Monitor.

One last important aspect involves attacker vs. defender precepts, which are often referred to as asymmetric. An attacker only needs to find one vulnerability to open the door and then work to expand exploitation, while the defender must effectively guard against all threat vectors based on the risk appetite and tolerances of individual organizations. Functional CRT/CSF functions for Cloud are further discussed below:

5.6.2.1. Cloud: Identify

CRT is defined within the scope of the "Identify" CSF function as the time needed for a data-owner organization to access available data from an asset service provider (i.e., through an API, command line, log form, etc.). This time can vary depending on the provider, service, and data, from 5 minutes up to 24 hours. This is cyber-relevant to the time taken for the identification and reconciliation of an information asset or set of assets. For example, hardware and software inventory updates, or ephemeral (short-lived) elastic service instances.

5.6.2.2. Cloud: Protect

CRT is defined within the scope of the "Protect" CSF function as the time needed for a data-owner organization and/or service provider to determine risk or threat level and implement risk mitigation(s). This is cyber-relevant to the time taken for the protection of an information asset or set of assets. For example, the application of operating system security patches.

5.6.2.3. Cloud: Detect

CRT is defined within the scope of the "Detect" CSF function as the time needed for a data-owner organization to ingest data from an service provider via API, Command line, logs, etc. This time can vary depending upon the structure of the data, tools in place for data ingestion, and whether the data is available to the data-owner organization from 5 minutes up to 24 hours. This is cyber-relevant to the time taken for the detection and reconciliation of situational status of an information asset or set of assets. For example, configuration setting updates and automated hardware and software inventory services.

5.6.2.4. Cloud: Respond

CRT is defined within the scope of the "Respond" CSF function as the time needed for a data-owner organization and/or service provider to respond to a cybersecurity event. This time can vary across organizations based upon available tools, infrastructure set-up, data back-up, and ability of an organization to respond. This is cyber-relevant to the time taken to respond to potential or actual compromise of an information asset or set of assets. For example, incident response and investigation of root cause analysis.

[9] NIST Risk Management Framework for Information Systems and Organizations, SP 800-37, revision 2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

5.6.2.5. Cloud: Recover

CRT is defined within the scope of the "Recover" CSF function as the time needed for a data-owner organization and/or service provider to recover from a cybersecurity event. This time can vary across organizations based on the ability of an organization to perform recovery functions and the tools available to the service provider. This is cyber-relevant to the time taken to achieve sufficient recovery from potential or actual compromise of an information asset or set of assets. For example, identify to recover actions are sufficiently achieved that minimize service disruption and meet business specific requirements and operational efficiencies.

6. DESIGN RECOMENDATIONS

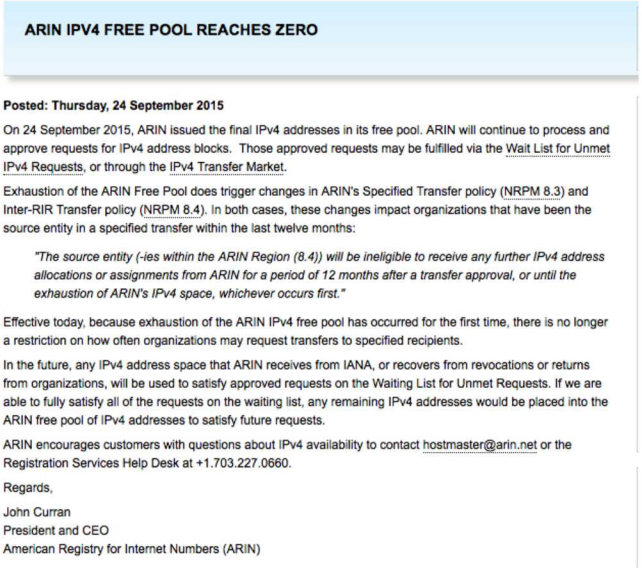
6.1. Design Planning

CPR design and the NIST CSF can be utilized in initial planning to strengthen critical infrastructure protection and cyber disruption response and recovery. An overall goal is to progress with newer standards-based technologies in new service areas. Technical investments should consider short (2-year), mid (5-year), and long-term (10-year) technical goals and business priorities. In many cases short and mid-year circumstances have already past. This is evident in the case of regional Internet registry IPv4 address exhaustion five years past and the IT/OT/IoT rollout currently underway in the IT and Communications sectors. National-Tribal analysis is intended to inform technical investments that may otherwise miss significant cost saving opportunities. The challenges and opportunities are evident in the great variety of technologies and community needs that need to be securely resolved.

Building with current standards-based technologies will result in long-term advantage for regional broadband network deployment, new service development, and ICS/SCADA security. Next steps include training, conducting preliminary CPR risk assessments followed by preemptive mitigations. Ongoing assessment of viable technologies and security concerns will be required overtime.

6.1.1. Internet Protocol

IPv4 address exhaustion has occurred worldwide and IPv6 is a distinctly different version that scales to vast growth. IPv4 address exhaustion for the North American Regional Internet Registry, American Registry for Internet Numbers (ARIN) is illustrated below.



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)

Figure 35. IPv4 Address Exhaustion 9-24-2015

IPv4 and IPv6 are fundamentally different in function and vastly different in scale. The current state in the IT and Communications sectors, and indeed the Internet, is IPv4 and IPv6 dual-stack dependence. It follows that moving to IPv6 only will reduce complexity by decommissioning IPv4. Risks and costs benefits may be realized in an IPv6 only infrastructure, which are enhanced with on CPR design practices and NIST CSF and RMF alignment. IPv6 deployment will require a knowledgeable workforce with the KSA necessary to design, secure, and maintain assurance across sectors and to manage inter-sector dependencies. Business partner and vendor collaboration is necessary for supply chain management and to realize fulsome economic and baked-in security gains.

Subsequent examples of Internet Protocol version differences are illustrated below.

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

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

Figure 36. Primary IPv4 IPv6 Differences

IP technologies are as relevant to critical infrastructure communications and protection.

6.1.2. Radio Frequency and Optical Communications

A mix of RF technologies is necessary for expanded broadband wireless and mobile communications in rural areas. Legacy cellular 3G/4G LTE and WiFi may be required in expanded service areas that have limited to technological access. TVWS may be useful to augment RF communications capabilities in such areas. 5G NR and WiFi6 may not be readily available or relevant to rural area deployment. Therefore, 5G NR technical investment planning should consider future development and the maturity of industry offerings.

Low Altitude Satellite Communications, or Low Earth Obit (LEO) are developing to increase broadband capability. A recent example is deployment by SpaceEx StarLink[10]. This illustrates that RF broadband communications continue to evolve. Therefore, planning should consider future development and the maturity of industry offerings overtime.

A mix of technologies may be necessary. Line of sight Infrared, Gigabit Passive Optical Networks (GPON), and 10Gb dense wave division multiplexing may be considered. Fiber to the home is an optimum but costly solution to be considered. RF and optical communications represent composite requirements in mobile wide area urban and rural communications. A similar consideration is the RF/IP coupling for fully functional mobile wide area urban and rural communications. RF and optical technologies are relevant to critical infrastructure communications and protection as well.

6.1.3. Data Center Virtualization

Information value and information asset protection are key considerations in the IT and Communications sectors. An enterprise datacenter offers the advantage of data owner-controlled infrastructure, and the disadvantage of high cost and maintenance. Data owner control is important when data sensitivity and value are high, as in the case of tribal government or personally identifiable information.

Cloud services offer cost benefit, although ICAM, IPAM, and information assurance must be balanced with cost and convenience. Service providers become integral partners for sufficient information assurance as data stewards in a supplier owned and operated infrastructure. Virtual services will continue to develop, including Cloud, AI, VR, AR, and SDN/NFV. Technical investments should consider future development and maturity of industry offerings overtime. Virtual technologies are as relevant to critical infrastructure communications and protection.

[10] https://spacenews.com/spacex-launches-second-batch-of-starlink-broadband-satellites/

7. INDUSTRIAL CONTROL SYSTEM SECURITY

The ICS security game has changed. Enterprise business networks (Level 5) couple with business unit or plant networks (Level 4) that couple with operation support networks through a DMZ[11]. Operation support networks are further defined at different levels: Level 3 - Operations Support; Level 2 -Supervisory Control LAN; Level 1 - Control Devices; and Level 0 - Process Control Instrumentation Bus Network. An ICS is further segmented into a Safety Zone, and finally, an Enforcement Zone, which is comprised of programmable logic controllers and control processors, sensors, actuators, and other instrumentation.

What has changed is the nature of connectivity, computation, and threat with the advent of IoT, Mobile IoT, and Industrial IoT instrumentation. There are two major considerations: First, the convergence of two distinctly different IT and OT ICS/SCADA workforce cultures that comprise divergent KSA[12]; and, Second, the convergence of distinctly different types of technology, IT and OT ICS/SCADA. ICS. OT ICS/SCADA systems inherently require a high-level of security, while IT is inherently insecure. National-Tribal CIP offers an approach to bridge this gap.

7.1. The NIST Special Publication 800-82, Revision 2

The NIST SP 800-82, Guide to ICS Security, May 2015, provides guidance for ICS and SCADA system security.

As relevant and valuable as this publication is, the challenge remains to secure ICS/SCADA critical infrastructure systems in the rapidly changing and expanding cyber-ecosystem. Not unlike many references, the document fails to illustrate IPv4 and IPv6 as uniquely different protocol stacks in the Digital Dichotomy, focusing rather on IP as a singular suite. The Sandia Labs Tribal Cyber-Energy team advises that the digital dichotomy be acknowledged in order to prepare a readily skilled workforce to sufficiently secure emergent ICS/SCADA systems.

7.2. The New Technological Paradigm

Consider the IoT renditions as instrumentation for critical infrastructure innovation. The most recognized example is Smart Grid, or rather modernized distributed Energy delivery systems. Energy comprises generation, transmission, storage, and load across vast areas that increasingly depend on renewable technologies at the same time as becoming increasingly connected and computerized. The Transportation sector is another prime example where automation is impacting “auto-motion” with automated self-driving vehicles with dedicated short-range wireless communications.

The new technological paradigm is based on scalable technologies. For example, years ago the business case for IPv6 was hard to make: Why add complexity risk and cost when IPv4 still worked fine? Today, the cyber-ecosystem has changed drastically: Broadband, OT/IT/IoT, and virtualization are demanded at scale with new applications, for example in Smart Agriculture. Recent studies have placed the Internet at 60 billion devices, yet we have not begun to realize the composite impact due to critical infrastructure modernization at scale. Essentially, we are at the beginning of this disruptive technological change. Hence, moving to scalable standards and technologies is mandated to meet the needs of the changing cyber-ecosystem.

A new perspective of disciplined security design is necessary, where collectively, CPR design, preemptive mitigations, and data-centric protection provide improved measures to avoid, eliminate, or contain vulnerabilities and strengthen critical infrastructure protection at the national scale. Therefore, National-Tribal CIP collaboration represents an unprecedented opportunity to bake-in security and establish positive control in the face of the critical infrastructure insecurity problem and increasing risk.

Cybersecurity is often considered to specialized and abstract to be a design requirement, yet it must be part of the critical infrastructure modernization conversation. Without it, the risk of compromise and potential loss of life is too high. We can and must do better through the power of National-Tribal collaboration. The most important factor is the human factor. Multi-stakeholder collaboration and a trained and ready workforce are required. Attacker/defender interplay is a prime concern, which can only be countered with the right KSA and situational awareness. National-Tribal CIP directly addresses these challenges with extraordinary benefits to national security.

---

[11] http://www.sans.org/ics

[12] SANS ICS/SCADA Security Essentials

8. INTEGRATED EMERGENCY, CONTINUITY, AND CYBER RESPONSE AND RECOVERY

The stakes have been raised with the onslaught of Information and Communications technological change coupled with the wholesale integration of IT with OT and IoT. It follows that Emergency Management, Business Continuity, and Cyber Disruption Response and Recovery should likewise evolve to the new technological paradigm. Concepts for modernized response and recovery are discussed herein.

Business Continuity Planning (BCP) is a program that assesses the existing operations, risks, and customer relationships of an organization for the development of organizational preparedness. This integrated Emergency Management, Business Continuity, and Cyber Disruption Response model develops an integrated approach for ensuring that critical processes continue to function during and after a disaster or incident that interrupts the operation of the organization and its business partners. The Homeland Security national incident management system/incident command system provides the basis for this BCP command structure.

An integrated command structure is designed to benefit the operational environment with coordinated emergency management (EM), Cyber Response and Recovery, which expands on the concept of IT disaster recovery (ITDR), continuity of operations planning (COOP), and collaborative information management. Roles have been assigned as they pertain to executive management and decision makers. Federated BCP elements are supported through a BCP COOP program office. The four elements provide core services to keep the organization in operation during time of crisis. Similarly, the finance and administration functional area has been added because of critical importance during BCP activation. The federated BCP command structure is illustrated below.

A culture of continuity event awareness is needed throughout the organization and leadership. This begins with CPR design comprised of preliminary risk and mitigation analysis embodied as initial design requirements and response and recovery considerations. Important areas of consideration include application security (AppSec), and OpSec to provide a stronger foundation for cyber disruption response planning.

Cyber Disruption Response in a Changing Cyber Ecosystem

CPR design is tied to all aspects of cyber disruption response planning. This is integral with critical infrastructure protection, where the IT and Communications critical infrastructure sectors foster innovation that impacts other critical infrastructure sectors.

Business continuity, CPR design, and cyber disruption response planning are coupled due to new dependencies, where IT, OT, IoT are being integrated at an astounding pace and scale. The new information and communication technology dependencies create opportunities and challenges.

The functional model presented is considered to be a distributed solution that provides responsiveness in any situation, and allows leadership and personnel to solve the problems at hand. The majority of recovery work will be done by operations teams under the direction of area Section Chiefs. The overall command structure is intended to facilitate consistency in approach and communications. Each incident is unique and requires evaluation of vulnerabilities and threats to determine appropriate action. Such a distributed solution should assist in dynamic response in the most difficult of times.

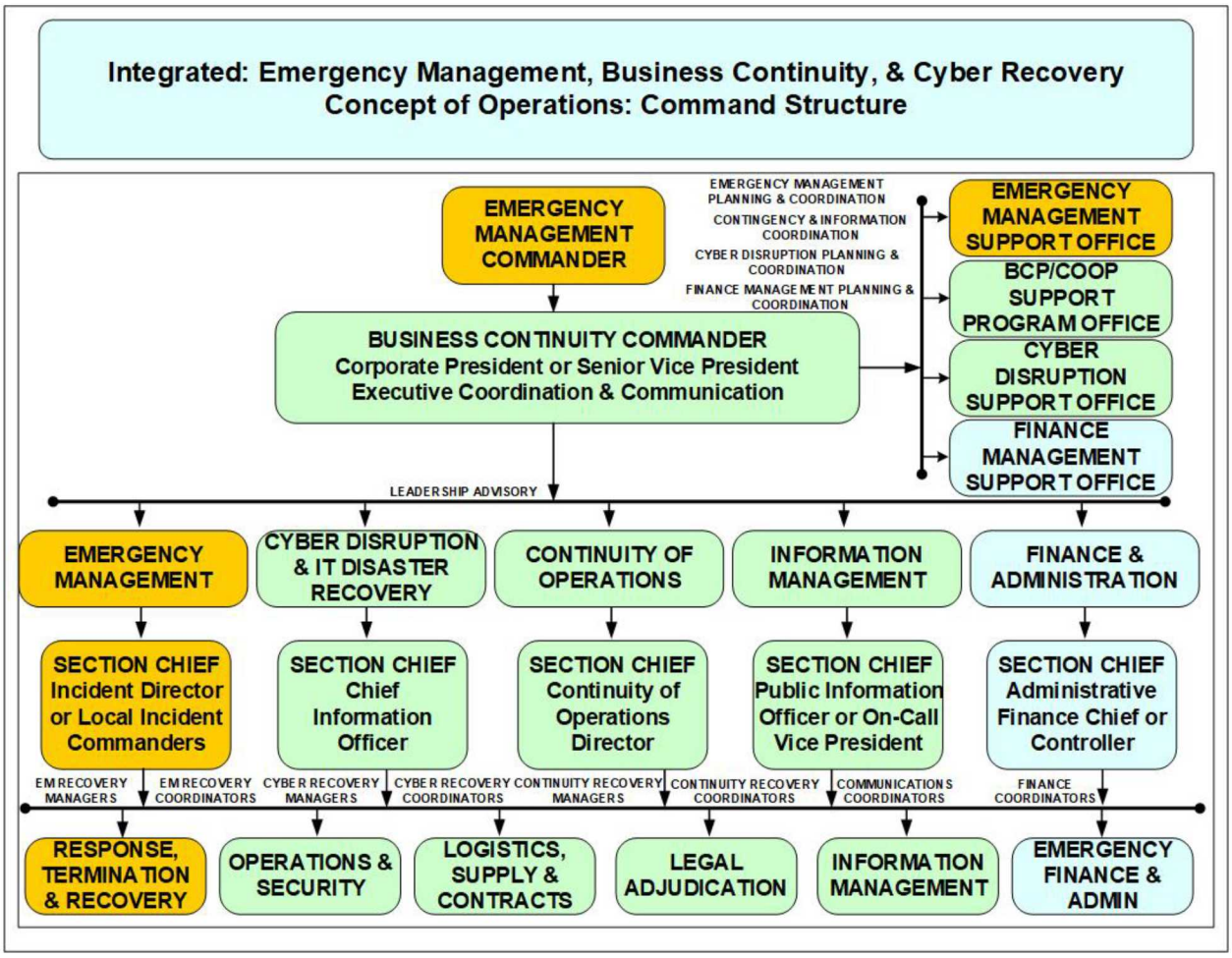


Figure 37. Integrated Emergency and Cyber Response and Recovery: Command Structure

Illustrated below is a concept for the coordination and overlap of EM and BCP facilitated through consistent executive, command, public, internal and external communications where vulnerabilities for each incident are examined. BCP activation is called for by the Business Continuity Commander when cleared by the Emergency Management Commander as safe to proceed.

When emergency management is not involved the Business Continuity Commander assumes full authority of recovery operations. Note that appropriate levels of physical and cyber security must be maintained throughout the BCP life cycle.

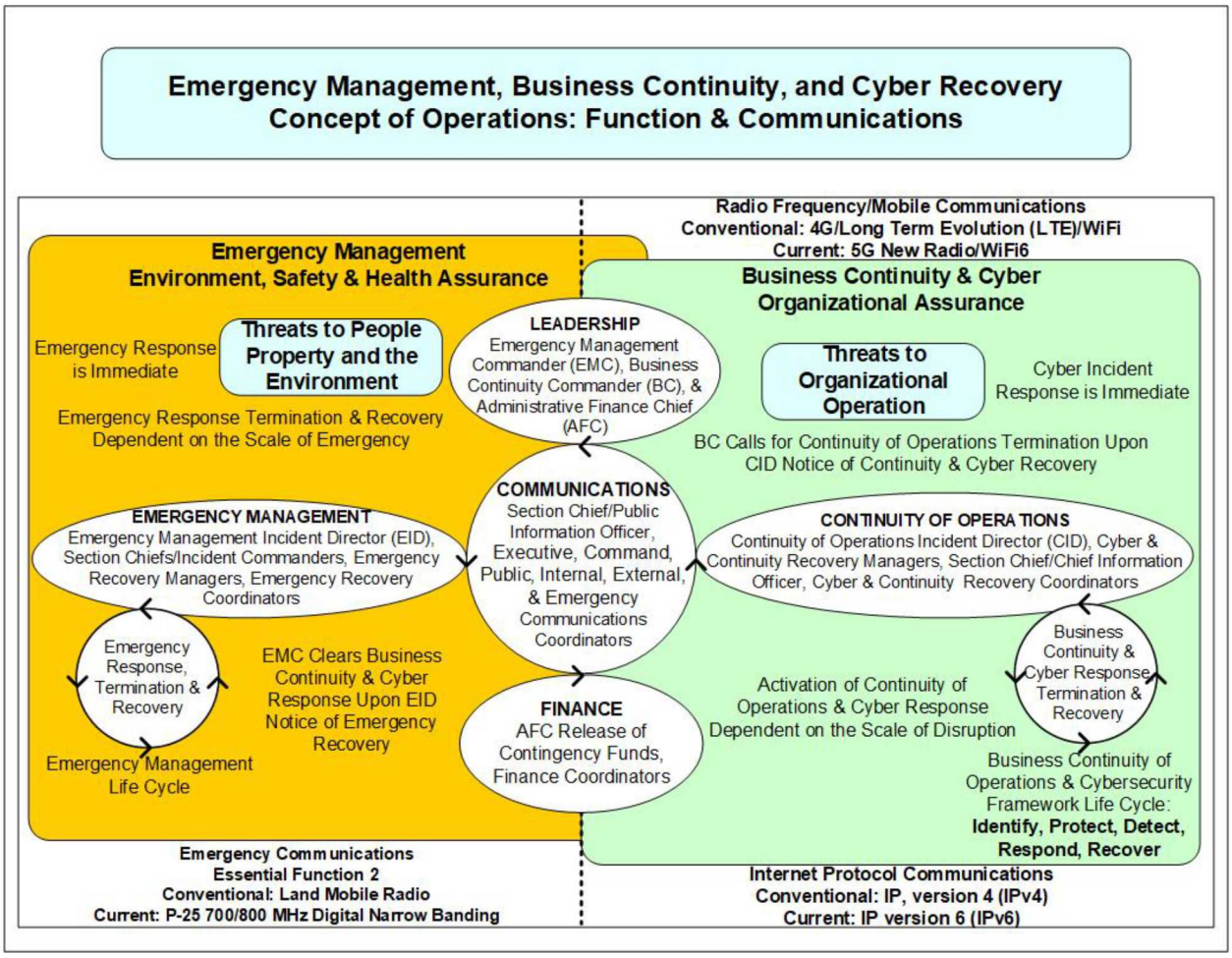


Figure 38. Integrated Emergency and Cyber Response and Recovery: Operations

BCP Conditions of Activation, Operation and Termination

Emergency operations have established methodologies for emergency response rooted in the national incident management system/incident command system. These include roles and activities that define initial emergency response (activation phase), resolution of the emergency situation (termination phase) and return to normal operations (recovery phase). BCP activation will work in-kind with EM, meaning that the Emergency Management Commander will have authority of control for the BCP activation and operation phases for all operations of the organization. The Emergency Incident Director will work with the Emergency Management Commander, the Incident Commanders and Section Chiefs to manage initial response through to the termination of the emergency situation. The emergency situation is terminated when threats and hazards to people, property and the environment are manageable, and a safe environment is restored. Upon the Business Continuity Commander's declaration of BCP activation, the COOP, Cyber Response and Recovery, information management operations (identify, protect, detect, respond, and recover) begin. The EM BCP Coordination Officer coordinates BCP operations with the Section Chiefs and the recovery teams (recovery manager and recovery coordinators). Executive, command, public, internal and external communications are coordinated with the Public Information Officer, Community of Interest Officer's and the BCP Coordination Officers as necessary.

BCP Conditions of Activation

BCP activation is triggered when an incident is determined to threaten mission operations. Threats to mission operations include: threats to work force personnel, property and the environment requiring emergency response; threats to critical infrastructure that are essential to the operation of the organization (facilities, energy

and water utilities, information and communication networks); threats to the operability of critical processes, supply chain and partnerships.

The Business Continuity Commander declares BCP activation to initiate resumption and recovery services and communication. BCP activation puts into action mission operation contingency plans in order to sustain critical processes and services with the release of contingency funds availability from the Administrative Finance Chief. The Business Continuity Commander works in coordination with the Emergency Management Commander when emergency management is necessary to restore a safe working environment. When the safety to people, property or the environment are threatened the Emergency Management Commander assumes authority for recovery operations. This an important consideration as situational awareness changes.

BCP Conditions of Operation

BCP operations initiate upon BCP activation as contingency plans and recovery operations begin. Contingency operations can run in conjunction with EM recovery operations through to completion of the BCP operations phase. Mission recovery includes the recovery of facilities, infrastructure and services required for the return to normal operations. The Business Continuity Commander declares that BCP operations are completed upon consensus from the Emergency Management Commander, BCP Coordination Officers, Leadership Advisory, Section Chiefs, Recovery Managers and Recovery Coordinators.

BCP Conditions of Termination

BCP operations can be terminated when facilities, infrastructure and services are sustainable and reliable. The Business Continuity Commander declares that normal operations may resume upon consensus from the Emergency Management Commander, BCP Coordination Officers, Leadership Advisory, Section Chiefs, Recovery Managers and Recovery Coordinators. The Administrative Finance Chief closes contingency funds availability and conducts cost recovery upon return to normal operations.

Critical Issues

BCP operations are dependent on planning, communication, coordination and security. Critical issues include:

1. Personnel Safety
2. Environmental Safety
3. Physical Security
4. Cyber Security
5. Resilience
6. Identification of Critical personnel
7. Identification of Critical assets
8. Identification of Critical processes
9. Identification of Vital Records
10. Established Command Structure
11. Managed Command Communications
12. Managed Public Information and Safety Communications
13. Managed EM and BCP Internal Communications
14. Prioritization of Activities
15. Training, Testing and Continual Improvement
16. Timely Implementation
17. Managed Internal Work Force Information and communications
18. Managed Telecommute Work Force Information and communications
19. Managed External Partner and Oversight Information and communications
20. Managed Legal Adjudication and Information Protection
21. Managed Contractual Obligations

Conceptual BCP Roles and Responsibilities

A variety of roles and responsibilities are discussed that are intended to represent local to wide-area integrated response.

- Emergency Management Commander (EMC) - The Emergency Management Commander is responsible for all emergency operations until threats and hazards to people, property and the environment are

terminated. The Emergency Management Commander is an assigned emergency management leadership position that owns the responsibility for executive decisions and communications.

- Emergency Incident Director (EID) – The Emergency Incident Director is responsible for all emergency operations coordination and communications and doubles as the emergency management area section chief. The Emergency Incident Director is in place to coordinate multiple ICs during large scale multi-site emergency management events.
- Incident Commander (IC) - An Incident Commander is responsible for on-site field emergency operations until threats and hazards to people, property and the environment are terminated. Incident Commander's report to the Emergency Incident Director and when necessary the Emergency Management Commander
- Business Continuity Commander (BC) - The Business Continuity Commander is responsible for overall BCP coordination and communications. The Business Continuity Commander declares BCP activation and termination in coordination with the Emergency Management Commander. The Business Continuity Commander is a leadership position that owns the responsibility for executive decisions and communications.
- COOP Incident Director (CID) – The COOP Incident Director is responsible for all COOP, including Cyber Response and Recovery operations, and coordination and communications and doubles as the COOP section chief. The COOP Incident Director is in place to coordinate multiple COOP coordinators across a wide area during large scale multiple site and organization continuity events.
- BCP Coordination Officer (PCO) – Each BCP Coordination Officer is responsible for facilitating planning and training activities in times of order and provides coordination across the enterprise and collaborative business partners during BCP activation. BCP Coordination Officer's report to the BCP program office and coordinate closely with the PIO, CoIO and members of the leadership advisory. BCP Coordination Officer's ensure consistency in development and application of resources across the organization.
- Public Information Officer (PIO) – The Public Information Officer is responsible for consistent and accurate public relations and safety communications.
- Community of Interest Officer (CoIO) - The Community of Interest Officer is responsible for business partner and oversight communication.
- Leadership Advisory (LA) – The Leadership Advisory is a designated group of corporate officers and section chiefs with the responsibility to provide accurate and truthful information to executive leadership. Critical corporate decisions for continuity, sustainability and survivability will rest with the Leadership Advisory.
- Administrative Finance Chief (AFC) – The Administrative Finance Chief is responsible for overall coordination of emergency and contingency expenditures and cost recovery.
- Section Chief (SC) – Each Section Chief is responsible for coordination of area activities and reporting of issues that require higher level attention to the Emergency Management Commander and Business Continuity Commander.
- Recovery Manager (RM) – Each Recovery Manager is responsible for their mission area recovery coordination, which includes the restoration of support services needed to perform mission during BCP operations and full recovery to normal operations.
- Recovery Coordinator (RC) - A Recovery Coordinator is responsible for supporting Recovery Managers by facilitating EM, COOP, Cyber Response and Recovery, and information management activities.

9. KEY TAKEAWAYS

In closing, Sandia Labs provides objective advisory for national and tribal critical infrastructure modernization, security, and resilience. The coupling of world-class science and engineering, interdisciplinary teaming, technical expertise, and objective advisory positions Sandia Labs as a ready National-Tribal CIP facilitator to the advantage of all stakeholders.

Federal sponsorship is needed for a National-Tribal CIP level-of-effort. Multiple federal sponsors potentially have stakeholder interest, including sector specific agencies. DHS/CISA, DOC/NTIA, NITRD/Broadband, DOE, and DOI/BIA current activities potentially benefit and can be greatly enhanced with National-Tribal CIP collaboration.

Current project-driven tribal levels-of-effort do not scale to provide benefits across tribal and associated national stakeholder concerns. The goal for this National-Tribal CIP proposed solution is fulsome future forward security and resilience. There are several key takeaways to consider in what may be a wholesale shift in the CIP paradigm, they include:

1. The National-Tribal CIP vision is to deliver extraordinary national security benefit to a full complement of federal and tribal stakeholders
2. Threat increases with an increased critical infrastructure IT/OT/IoT attack surface
3. Divestiture of legacy technologies provides a means to reduce complexity, risk, and cost, thereby reducing the digital dichotomy attack surface
4. Moving to scalable standards-based technologies provides an opportunity to increase critical infrastructure security posture and increase cyber disruption response and recovery capabilities
5. Disciplined CPR design practices provide a means to bake-in security in new build opportunities
6. Data-Centric protection provides a means to better secure information assets based on the value of information and how information assets are accessed and by whom (user accounts) or what (service accounts) as mobility and virtualization create a data-everywhere, user-anywhere paradigm with no defined network perimeter
7. Preliminary risk assessments provide a means to raise the protection posture at the onset of design, thereby informing preemptive critical infrastructure mitigations
8. Preemptive critical infrastructure mitigations resulting from preliminary risk assessments should include ICAM and OSS protection mechanisms
9. R&D could include metrics to better detect and validate indicators of compromise with MTTD, $MTTR^s$ and $MTTR^c$
10. Integrated EM, BCP, and Cyber disruption and response provide a means for integrated response and recovery to cyber disruptive events
11. Advancing a capable workforce requires trained, certified, educated, and qualified STEM professionals skilled in current and scalable technologies
12. National-Tribal CIP as an unprecedented collaboration opportunity to address national and tribal critical infrastructure priorities with extraordinary national security benefits for improved measures to avoid, eliminate, or contain critical infrastructure vulnerabilities and reduce threat exposure

ACRONYMS AND DEFINITIONS

Organizational	Definition
AI/AN	American Indian and Alaskan Native
ARIN	American Registry for Internet Numbers
BIA	Bureau of Indian Affairs
BIE	Bureau of Indian Education
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DMTF	Distributed Management Task Force
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of Interior
FCC	Federal Communications Commission
IEC	International Elecrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standards
MRGTPC	Middle Rio Grande Tribal Pueblo Consortium
NATA	Native American Telecom Association
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NMSBA	New Mexico Small Business Assistance
NNSA	National Nuclear Security Administration
NTIA	National Technology and Information Administration
NTTA	National Tribal Telecom Association
SLTT	State, Local, Tribal, and Territorial
THSGP	Tribal Homeland Security Grants Program
USG	United States Government
WGA	Western Governors Association
WRP	Western Regional Partnership (Energy)

Training/Edu	Definition
ABET	Accreditation Board for Engineering and Technology
AIHEC	American Indian Higher Education Consortium
AMNI	Advanced Manufacturing Network Initiative
BMCC	Bay Mills Community College
CCCC	Cankdeska Cikana Community College
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CECOR	Consortium Enabling Cybersecurity Opportunities and Research
CFCE/CCE	Certified Forensic Computer Examiner & Certified Computer Examiner
CIESESE	Consortium for Integrating Energy Systems in Engineering and Science Education
CISSP	Certified Information System Security Professional (ISC^2)
ESRI	Enterprise Security Risk Management (ASIS)
GIAC	Global Information Assurance Certification (SANS)
GCIH	GIAC Certified Incident Handler (SANS)
GPEN	GIAC Certified Penetration (PEN) Tester (SANS)
GXPEN	GIAC Exploit Researcher and Advanced Penetration Tester
HBCU	Historically Black Colleges and Universities
ISC^2	International Information Systems Security Certification Consortium
KSA	Knowledge, Skills, and Abilities
MCSE/P	Microsoft Certified Solutions Expert/Professional
MSI	Minority Serving Institutions
MSIPP	Minority Serving Institution Partnership Programs
NMSU	New Mexico State University
NMSU	New Mexico State University
NMT	New Mexico Tech
NTU	Navajo Technical University
OSCP	Offensive Security Certified Penetration Tester
RHCSA	Red Hat Certified System Administrator
SANS	SysAdmin, Audit, Network, Security Institute
SFIS	Santa Fe Indian School
SIPI	Southwest Indian Polytechnic Institute
SKC	Salish Kootenai College
TCU	Tribal Colleges and Universities
TMCC	Turtle Mountain Community College
UNM	University of New Mexico

Technical	Definition
2G	Second Generation of cellular mobile communications (Voice)
3G	Third Generation of cellular mobile communications (Data)
3GPP	Third Generation Partnership Project
4G	Fourth Generation of cellular mobile communications (Video)
5G	Fifth Generation of cellular mobile communications (Broadband)
5G NR	Fifth Generation New Radio
A	DNS Address Record (IPv4)
AAAA	DNS Quad Address Record (IPv6)
ACL	Access Control List
AAD	Azure Active Directory
AD	Active Directory
AES	Advanced Encryption Standard
AFC	Administrative Finance Chief
AI	Artificial Intelligence
AIC^2IA	Availability, Integrity, Confidentiality (OT) – Confidentiality, Integrity, Availability (IT)
AIDE	Advanced Intrusion Detection Environment
API	Application Programming Interface
AppSec	Application Security
AR	Augmented Reality
ARP	Address Resolution Protocol (IPv4)
BCC	Business Continuity Commander
BCO	BCP Coordination Officer
BCP	Business Continuity Planning
CDM	Continuous Diagnostics and Mitigation
CID	COOP Incident Director
CIM	Common Information Model
CIP	Critical Infrastructure Protection
COOP	Continuity of Operations Planning
CoIO	Community of Interest Officer
CPR	Cyber-Physical-Resilient Design
CRT	Cyber-Relevant Time
CSF	Cyber Security Framework (NIST)
CSMA	Carrier Sense Multiple Access
CSP	Cloud Service Provider
DHCP	Dynamic Host Configuration Protocol
DN	Domain Name
DNS	Domain Name System
EaaS	Email as a Service

Technical	Definition
EID	Emergency Incident Director
EISP	Enterprise Information Security Policy
EHF	Extremely High Frequency
EM	Emergency Management
EMC	Emergency Management Commander
FAN	Field Area Network
FISMA	Federal Information Security Management Act
GCP	Google Cloud Platform
GMF	Government Master File
GSDS	Google Suite Directory Sync
HPC	High Performance Computing
IaaS	Infrastructure as a Service
IC	Incident Commander
ICAM	Identity, Credential, and Access Management
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IDART	Information Design Assurance Red Team
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IMAP	Internet Message Access Protocol
IoT	Internet of Things
IP	Internet Protocol
IPAM	Internet Protocol Address Management (IPv4 and IPv6)
IPv4	Internet protocol, version 4
IPv6	Internet protocol, version 6
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISP	Internet Service Provider
ISSP	Issue-Specific Security Policy
IT	Information Technology
ITDR	Information Technology Disaster Recovery
LA	Leadership Advisory
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMR	Land Mobile Radio
LEO	Low Earth Orbit
MAC	Media Access Control
MFA	Multifactor Authentication
MIoT	Mobile Internet of Things
ML	Machine Learning

Technical	Definition
MTTD	Mean Time to Detect
$MTTR^s$	Mean Time to Respond
$MTTR^c$	Mean Time to Recover
NCPS	National Cybersecurity Protection System
NDP	Neighbor Discovery Protocol (IPv6)
NFV	Network Function Virtualization
NOC	Network Operations Center
O365	Microsoft Office 365
OFDM	Orthogonal Frequency Division Multiplexing
OOB	Out of Band
OPSEC	Operational Security
OSS	Operational Support Systems
OT	Operational Technology
PIO	Public Information Officer
PSAP	Public Safety Answering Point
P-25	Project 25
PaaS	Platform as a Service
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POP3	Post Office Protocol 3
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RC	Recovery Coordinator
RF	Radio Frequency
RFID	Radio Frequency Identification Devices
RIPTIDE	Resilient Infrastructure Protection Technical Interdisciplinary Expertise
RM	Recovery Manager
RMF	Risk Management Framework (NIST)
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SC	Section Chief
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDN	Software Defined Network
SDR	Software Defined Radio
SHF	Super High Frequency
SLA	Service Level Agreement
SLAAC	Stateless Address Autoconfiguration (IPv6)

Technical	Definition
SMTP	Simple Message Transport Protocol
SOC	Security Operations Center
SPP	Strategic Partnership Project
SSID	Service Set Identifier
SSO	Single Sign-On
SysSP	System Security Plan
TVWS	Television White Space
UHF	Ultrahigh Frequency
ULS	Universal Licensing System
URL	Universal Resource Locator
USB	Universal Service Bus
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VR	Virtual Reality
WAN	Wide Area Network
WEP	Wireless Equivalent Privacy
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

REFERENCES

Technical

Internet Engineering Task Force (IETF) Request For Comment (RFC) 8200 Internet Protocol, Version 6 (IPv6) Specification, July 2017: https://tools.ietf.org/html/rfc8200

IETF RFC 4291 IP Version 6 Addressing Architecture, February 2006: https://tools.ietf.org/html/rfc4291

IETF draft-ietf-opsec-v6-14

American Registry for Internet Numbers (ARIN) IPv4 Address Exhaustion: https://www.arin.net/vault/announcements/2015/20150924.html

5G Cybersecurity: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

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

5G World Alliance: http://www.5gworldalliance.org/

Third Generation Partnership Project: https://www.3gpp.org/

5G NR: https://www.lawfareblog.com/lawfare-podcast-tom-wheeler-need-real-cybersecurity-5g

Amazon Web Services: https://acloud.guru/learn/aws-ipv6

FCC TAC Securing SDN-NFV, December 2016: https://www.fcc.gov/oet/tac/2016

National Institute of Standards and Technology (NIST) FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, FIPS 199, February 2004: https://csrc.nist.gov/publications/detail/fips/199/final

NIST SP 800-37 Rev 2, Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy, December 2018: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

NIST Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018: https://www.nist.gov/cyberframework

NIST SP 800-12: An Introduction to Computer Security: The NIST Handbook: https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final

NIST SP 800-14: Generally Accepted Security Principles and Practices for Securing Information Technology Systems: https://csrc.nist.gov/publications/detail/sp/800-14/archive/1996-09-03

NIST SP 800-15: Technical Guide to Information Security Testing: https://csrc.nist.gov/publications/detail/sp/800-115/final

NIST SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems: https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

NIST SP 800-30: Risk Management Guide for Information Technology Systems: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

NIST SP 800-53 Rev. 3: Recommended Security Controls for Federal Information Systems and Organizations: https://nvd.nist.gov/800-53

NIST SP 800-171r1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations [including updates as of 11-28-2017]: https://doi.org/10.6028/NIST.SP.800-171r1

NIST SP 800-82, Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015: https://doi.org/10.6028/NIST.SP.800-82r2

NIST SP 800-160v2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach, November 2019: https://doi.org/10.6028/NIST.SP.800-160v2

NIST SP 1800-19B, preliminary-draft Trusted Cloud: Draft SP 1800-19 Volume B, "Approach, Architecture, and Security Characteristics": https://csrc.nist.gov/publications/detail/sp/1800-19/draft

Gartner Solution Comparison of the IAM Capabilities Within AWS, Azure and GCP

GAO-703193 Cloud Computing Security, December 2019: https://www.gao.gov/products/GAO-20-126

GAO-19-332, CRITICAL INFRASTRCTURE PROTECTION/ Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid – 701079, August 2019: https://www.gao.gov/products/GAO-19-332

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES: Completing the Transition to Internet Protocol Version 6 (IPv6), March 2020

ASIS Internationals Enterprise Security Risk Management (ESRI): https://www.asisonline.org/publications--resources/news/press-releases/asis-releases-new-enterprise-security-risk-management-esrm-guideline/

International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC)17799: https://www.iso.org/standard/39612.html

ISO and IEC 27002: https://www.iso.org/standard/54533.html

The Department of Energy Handbook for OPSEC, DOE-HDBK-1233-2019 June 2019

190613 DOE Cloud Smart Reference Guide (v2.0)

Guide to Firewalls and VPN's, 3rd Edition, Section B

Sandia National Laboratories

SAND2010-4766 National Cyber Defense and High Performance Computing Analysis-Concepts Planning Roadmap

SAND2014-5032 Cyberspace Modernization IP Planning Advisory

SAND2015-10336 PE NSTAC Big Data

SAND2016-11060 O NTIA IPv6 Implementation Comments

SAND2019-2304 TR Information Infrastructure Brainstorming Session

SAND2019-11978 C 5G-IPv6 Changing the Cyber-Ecosystem

SAND2019-12174 PE Changing Cyber-Ecosystem

SAND2019-15063 R Integrated Cyber Disruption Planning

Tribal Government Engagement Review

William S. Belko, "John C. Calhoun and the Creation of the Bureau of Indian Affairs: An Essay on Political Rivalry, Ideology, and Policymaking in the Early Republic," The South Carolina Historical Magazine 105, no. 3 (2004), p. 194: http://www.jstor.org/stable/27570693

July 9, 1832, ch. 174, §1, 4 Stat. 564.

Bureau of Indian Affairs (BIA) by Secretarial Order No. 2362.

Bureau of Indian Affairs (BIA), "About Us,": https://www.bia.gov/about-us

CRS Report RL34205, Indian Elementary- Secondary Education: Programs, Background, and Issues, by Cassandria Dortch.

BIA, "What We Do," at https://www.bia.gov/bia/ots/what-we-do

DOI, Indian Affairs, Budget Justifications Fiscal Year 2008, pp. IA-EDUC-5 to -6.

DOI, Indian Affairs, Budget Justifications and Performance Information Fiscal Year 2019, pp. IA-GS-1.

BIA, "Regional Offices": https://www.bia.gov/regional-offices

34 OPM Fedscope - The Indian Affairs Shutdown Contingency Plan—December 2018

Other

Other references as noted within the content of this document.