Integrated Emergency, Continuity, and Cyber Disruption Planning

The stakes have been raised with the onslaught of Information and Communications technological disruptive change coupled with wholesale integration of Information Technologies (IT) with Operational Technologies (OT). Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are now virtualized, automated, computerized and connected. Examples include Smart Grid and Smart Metering in the Energy sector; Automated Self Driving Vehicles in the Transportation Systems sector; ICS/SCADA modernization in the Water and Wastewater Systems sector; and Telemedicine in the Healthcare and Public Health sector. Vast broadband expansion brings new connectivity to rural and tribal communities with impacts to business, education, anchor institutions, and first responders.

Cyber innovation in the IT and Communications sectors is driving modernization across other Department of Homeland Security (DHS) defined critical infrastructure sectors.

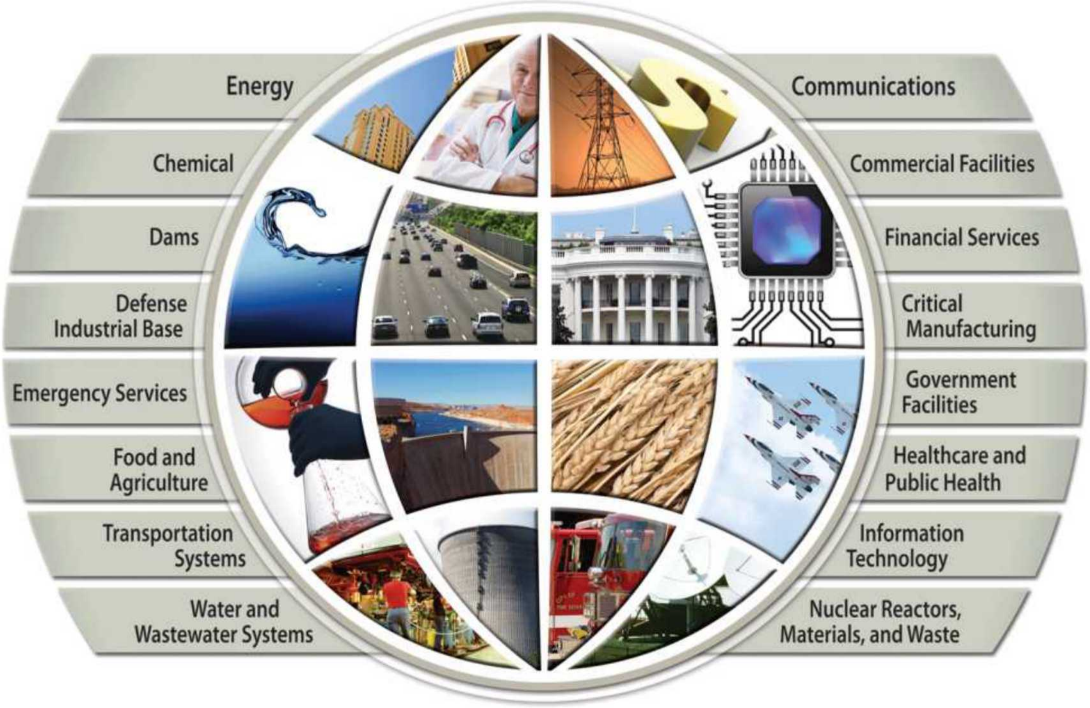


Figure 1. Department of Homeland Security Defined Critical Infrastructure Sectors

A high-level critical infrastructure protection perspective and rapid change motivates wide-area integrated emergency, continuity, and cyber disruption planning. This report provides a means of integrated emergency management, business continuity, and cyber disruption response and recovery aligned with the National Institute of Standards and Technology (NIST) cybersecurity framework and current standards-based technologies.

"*When our plan meets the world, we must adapt.*" Captain "Sully" Sullenberger

Alignment with the NIST Cybersecurity Framework reflects national critical infrastructure protection efforts. The NIST Cybersecurity Framework core functions: Identify, Protect, Detect, Respond, and Recover are illustrated in Figure 2.

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-NA-0003525.

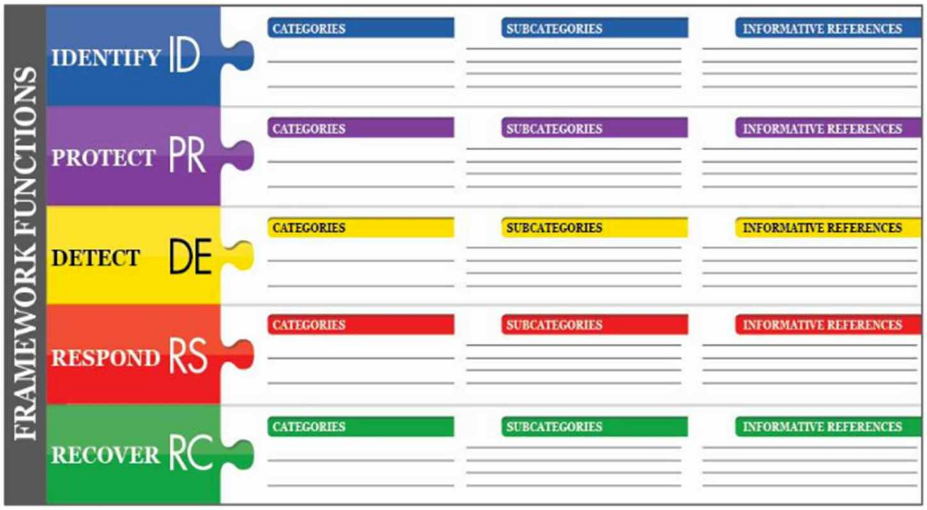


Figure 2. NIST Cybersecurity Framework Core

The Changing Cyber Ecosystem

A state of codependence on conventional and current standards is inherent in the IT and Communication sectors. Internet Protocol, version 6 (IPv6), Fifth Generation New Radio (5G NR), WiFi6, and Project 25 (P-25) represent next generation technologies that are not backwards compatible with predecessor technologies, as illustrated in Table 1.

Standards Body	Conventional	Current	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	P-25 700-800Mhz Digital Narrow Banding	Digital Two-Way Radio with Encryption

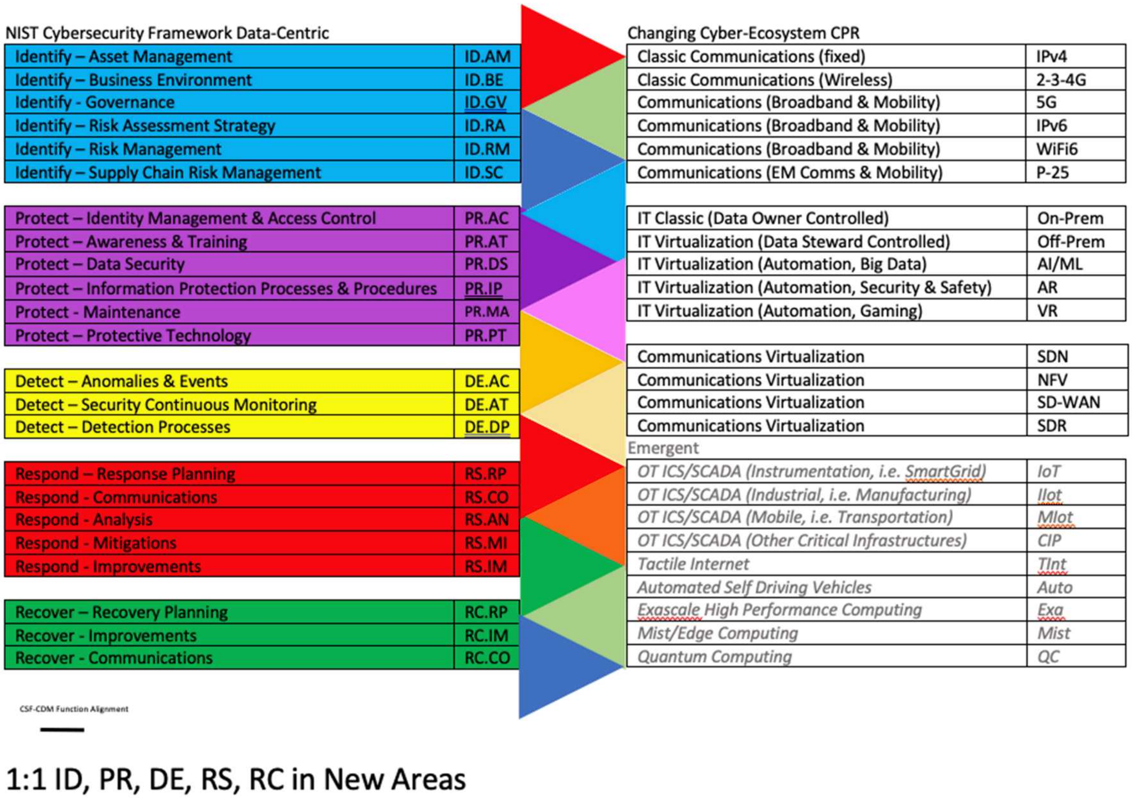
Table 1. Dichotomy of Legacy and Current Technologies

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

The Land Mobile Radio to P-25 transition further complicates emergency communications.

The Internet of Things (IoT) can be viewed as facilitating the instrumentation for modernized ICS/SCADA systems, which then become critically dependent on current standards for function and scale. From this perspective, the IoT can be referenced as the instrumentation for Smart Grid and Smart Metering. IPv6 and 5G NR provide an underpinning for such instrumentation with regard to the IoT.

Figure 3. illustrates alignment of the NIST Cybersecurity Framework in the changing cyber ecosystem. CPR refers to cyber-physical-resilient design requirements.



NIST Cybersecurity Framework Data-Centric

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

Changing Cyber-Ecosystem CPR

Classic Communications (fixed)	IPv4
Classic Communications (Wireless)	2-3-4G
Communications (Broadband & Mobility)	5G
Communications (Broadband & Mobility)	IPv6
Communications (Broadband & Mobility)	WiFi6
Communications (EM Comms & Mobility)	P-25
IT Classic (Data Owner Controlled)	On-Prem
IT Virtualization (Data Steward Controlled)	Off-Prem
IT Virtualization (Automation, Big Data)	AI/ML
IT Virtualization (Automation, Security & Safety)	AR
IT Virtualization (Automation, Gaming)	VR
Communications Virtualization	SDN
Communications Virtualization	NFV
Communications Virtualization	SD-WAN
Communications Virtualization	SDR
Emergent	
OT ICS/SCADA (Instrumentation, i.e. SmartGrid)	*IoT*
OT ICS/SCADA (Industrial, i.e. Manufacturing)	*IIot*
OT ICS/SCADA (Mobile, i.e. Transportation)	*MIot*
OT ICS/SCADA (Other Critical Infrastructures)	*CIP*
Tactile Internet	*TInt*
Automated Self Driving Vehicles	*Auto*
Exascale High Performance Computing	*Exa*
Mist/Edge Computing	*Mist*
Quantum Computing	*QC*

CSF-CDM Function Alignment

1:1 ID, PR, DE, RS, RC in New Areas

Figure 3. NIST Cybersecurity Framework Alignment with the Changing Cyber-Ecosystem

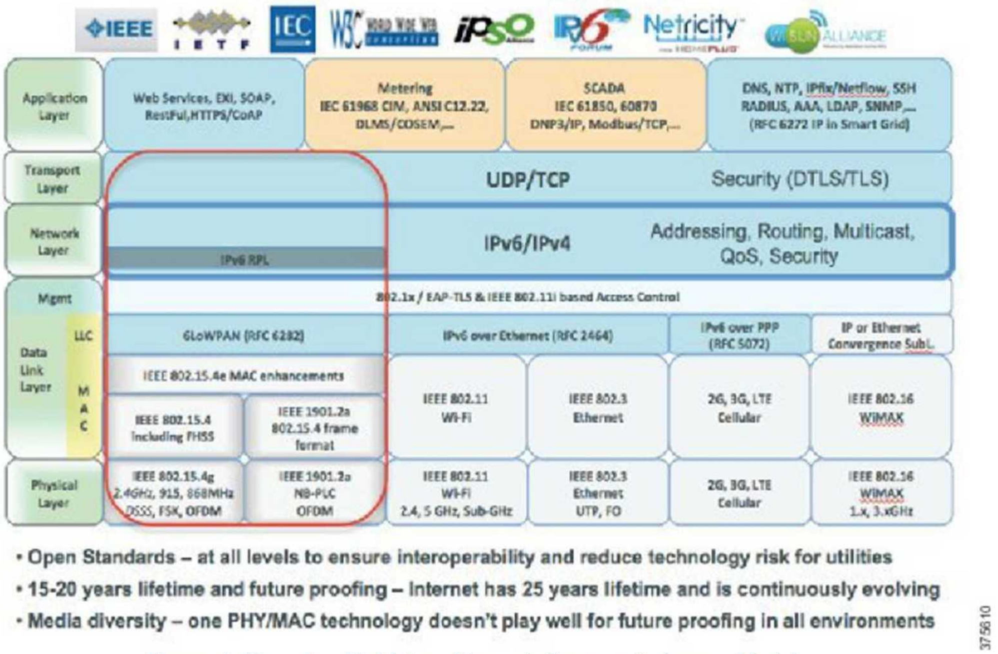
Virtualization has changed conventional data center deployment to Cloud service provider (CSP) data steward services. Virtualization includes virtual reality, machine learning and artificial intelligence. Table 2. illustrates conventional data center versus cloud technology practices.

Information Technology	Deployment	Capability	Constraint
Conventional Technology	Data Centers, Data Owner Controlled	On-Premises Co-located Data Access and Management, Enterprise Security	Data Center Physical and Environmental Costs
Current Technology	Cloud Services, Data Steward Controlled	Off-Premises Provisioning /Deprovisioning, Distributed Interorganizational Security	Loss of Data Centralization

Table 2. Data Center vs Cloud Services

Understanding and securing the current technological basis is essential to critical infrastructure protection for all stakeholders, which include national, state, tribal, territorial, local, and private sector interests.

An Energy Field Area Network Common Reference Model provides an example of integrated Energy IT/OT with current standards-based technologies, as illustrated in Figure 4. Note that Figure 4 omits 5G NR and WiFi6 standards, which implies additional technological impacts.


IEEE
IETF
IEC
W3C World Wide Web Consortium
IPSO Alliance
IPv6 Forum
Netricity HomePlug
Wi-SUN Alliance
Application Layer
Web Services, EXI, SOAP, RestFul,HTTPS/CoAP
Metering IEC 61968 CIM, ANSI C12.22, DLMS/COSEM,...
SCADA IEC 61850, 60870 DNP3/IP, Modbus/TCP,...
DNS, NTP, IPfix/Netflow, SSH RADIUS, AAA, LDAP, SNMP,... (RFC 6272 IP in Smart Grid)
Transport Layer
UDP/TCP
Security (DTLS/TLS)
Network Layer
IPv6 RPL
IPv6/IPv4
Addressing, Routing, Multicast, QoS, Security
Mgmt
802.1x / EAP-TLS & IEEE 802.11i based Access Control
Data Link Layer
LLC
MAC
6LoWPAN (RFC 6282)
IPv6 over Ethernet (RFC 2464)
IPv6 over PPP (RFC 5072)
IP or Ethernet Convergence Subl.
IEEE 802.15.4e MAC enhancements
IEEE 802.15.4 including FHSS
IEEE 1901.2a 802.15.4 frame format
IEEE 802.11 Wi-Fi
IEEE 802.3 Ethernet
2G, 3G, LTE Cellular
IEEE 802.16 WiMAX
Physical Layer
IEEE 802.15.4g 2.4GHz, 915, 868MHz DSSS, FSK, OFDM
IEEE 1901.2a NB-PLC OFDM
IEEE 802.11 Wi-Fi 2.4, 5 GHz, Sub-GHz
IEEE 802.3 Ethernet UTP, FO
2G, 3G, LTE Cellular
IEEE 802.16 WiMAX 1.x, 3.xGHz
375810

- Open Standards – at all levels to ensure interoperability and reduce technology risk for utilities
- 15-20 years lifetime and future proofing – Internet has 25 years lifetime and is continuously evolving
- Media diversity – one PHY/MAC technology doesn't play well for future proofing in all environments

Figure 4. Cisco Inc. Field Area Network Common Reference Model

"*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,…*" 5G World Alliance (5GWA)

Cybersecurity Principals and Perspectives

IT cybersecurity design principles have long been established as: Confidentiality as a priority, Integrity as a necessity, and Availability as a necessity. These principals can also be applied to OT cybersecurity in a different order of precedence: Availability as a priority, Integrity as a necessity, and Confidentiality as a necessity. Together these add to the foundation for integrated OT/IT cyber-physical-resilient (CPR) design.

- IT Design Example:
    - Confidentiality (C) – Data encryption at Rest, In Transit, In Process
    - Integrity (I) – Validation, Authorization, Authentication, Audit, Accounting
    - Availability (A) – Virtual, Multisource, Multipath, Redundancy, Portability, Staffing, Skills Development

- OT Design Example:
    - Availability (A) – Safety and security systems and services: Virtual, Multisource, Multipath, Redundancy, Portability, Staffing, Skills Development
    - Integrity (I) – Validation, Authorization, Authentication, Audit, Accounting
    - Confidentiality (C) – Operations, safety and security support systems, back office financial and billing, data encryption at Rest, In Transit, In Process

Telecommunication services may follow the OT-AIC security architecture while back office operations follow the IT-CIA security architecture. The combined IT/OT cybersecurity architectures can be referred to as “AIC^{2}IA”, where confidentiality bridges IT/OT cybersecurity.

Information assets may be considered from another protection perspective that’s applicable when information moves from a data-owner controlled infrastructure to a data-steward controlled infrastructure, such as with a CSP.

- Information Asset Protection Example
    - Identity, including user and service entity account permissions
    - Operational support systems (OSS) data (IT-CIA, OT-AIC)
    - Data sensitivity and value
    - Data ownership / data stewardship responsibility
    - Data residence and location (on-premises, off-premises)
    - Information In-Process, In-Transit, At-Rest
    - Control Plane, Management Plane, Data Plane

The advantage to be taken is preemptively built secure systems from the onset of design.

Cyber Physical Resilient Design
Sustainable advantages can be realized by building securely in the early deployment of new build technologies. Advantage can be gained through concept to disposition early cyber, physical, and resilient threat and hazard mitigation as design requirements. Preemptive risk assessments may then be used to address technical, administrative, operational, manmade, and natural hazards.

CPR design presents an opportunity to get in front of the cybersecurity challenge rather than chasing it. Important areas of consideration include application security (AppSec), and operational security (OpSec) to provide a strong foundation for software defined services.

CPR design provides a distinct leap-ahead opportunity in heretofore unserved and underserved areas that have an historic under investment in older technologies. The benefit is preemptive security in a more consistent transition to new technologies as compared to a forklift transition for well-served areas the must move from heavy dependencies in conventional technologies.

There are two reasons for the technological dichotomy of IT/OT, Communications, and IoT divergence, which has significant impact to critical infrastructure protection:

1) Conventional standards cannot scale and accommodate expanding needs;

2) Current standards do scale and include capacity and capability that differs enough that they become incompatible with conventional standards.

Preemptive CPR design builds-in early and ongoing cyber threat mitigation, physical threat mitigation, and resilient hazard mitigation. Preemptive mitigation raises the security posture bar to meet the rise in rapid technological disruptive change.

Emergency, Continuity, and Cyber Disruption Response and Recovery

Business Continuity Planning (BCP) is a program that assesses the existing operations, risks, and customer relationships for the development of organizational preparedness. Critical people, processes, resources, services, and applications must be identified for each organization. Impacts of maximum tolerable disruption may then be identified.

Integrated emergency management, business continuity, finance, and cyber disruption response and recovery elements are supported through subsequent program offices. The four offices provide core services to keep the organization in operation during time of crisis. A proposed integrated command structure is illustrated in figure 5.

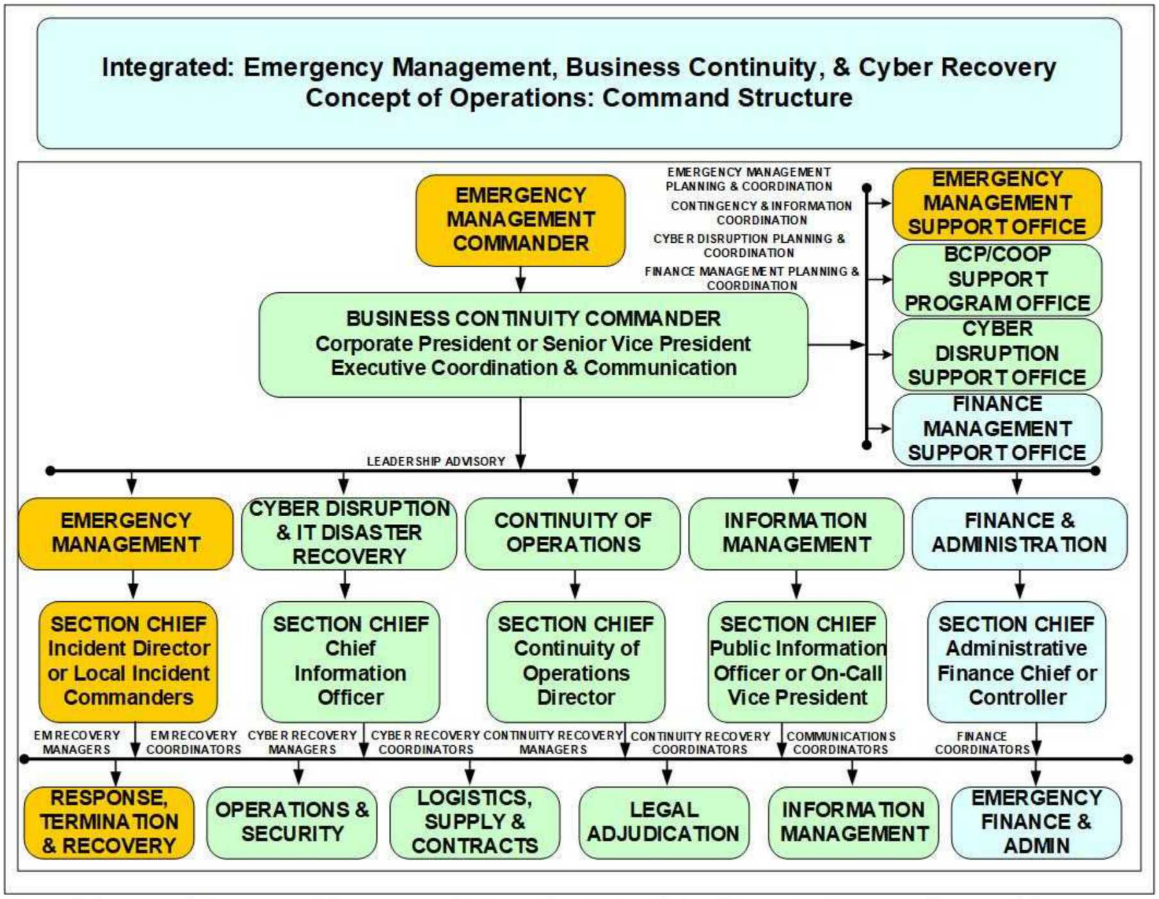

Integrated: Emergency Management, Business Continuity, & Cyber Recovery
Concept of Operations: Command Structure
EMERGENCY MANAGEMENT COMMANDER
EMERGENCY MANAGEMENT PLANNING & COORDINATION
CONTINGENCY & INFORMATION COORDINATION
CYBER DISRUPTION PLANNING & COORDINATION
FINANCE MANAGEMENT PLANNING & COORDINATION
EMERGENCY MANAGEMENT SUPPORT OFFICE
BCP/COOP SUPPORT PROGRAM OFFICE
CYBER DISRUPTION SUPPORT OFFICE
FINANCE MANAGEMENT SUPPORT OFFICE
BUSINESS CONTINUITY COMMANDER
Corporate President or Senior Vice President
Executive Coordination & Communication
LEADERSHIP ADVISORY
EMERGENCY MANAGEMENT
CYBER DISRUPTION & IT DISASTER RECOVERY
CONTINUITY OF OPERATIONS
INFORMATION MANAGEMENT
FINANCE & ADMINISTRATION
SECTION CHIEF Incident Director or Local Incident Commanders
SECTION CHIEF Chief Information Officer
SECTION CHIEF Continuity of Operations Director
SECTION CHIEF Public Information Officer or On-Call Vice President
SECTION CHIEF Administrative Finance Chief or Controller
EM RECOVERY MANAGERS
EM RECOVERY COORDINATORS
CYBER RECOVERY MANAGERS
CYBER RECOVERY COORDINATORS
CONTINUITY RECOVERY MANAGERS
CONTINUITY RECOVERY COORDINATORS
COMMUNICATIONS COORDINATORS
FINANCE COORDINATORS
RESPONSE, TERMINATION & RECOVERY
OPERATIONS & SECURITY
LOGISTICS, SUPPLY & CONTRACTS
LEGAL ADJUDICATION
INFORMATION MANAGEMENT
EMERGENCY FINANCE & ADMIN

Figure 3. Integrated Emergency Management, Business Continuity, Cyber Disruptive Response Command Structure

The integrated command structure is considered a distributed solution that provides responsiveness and situational awareness for wide-area complex incident management. Each incident is unique and requires evaluation of vulnerabilities, threats, and exposure to determine appropriate action. The majority of recovery work will be done by response and recovery teams under the direction of area Section Chiefs. The overall command structure is intended to facilitate consistency in approach and communications.

Figure 6 illustrates a proposed overlap and coordination of emergency management, business continuity, and cyber disruption response and recovery. Business continuity and cyber disruption response activation follows the Emergency Management declaration that hazards to people, property, and environmental are managed and it is safe to proceed with business continuity and cyber response and recovery activities.

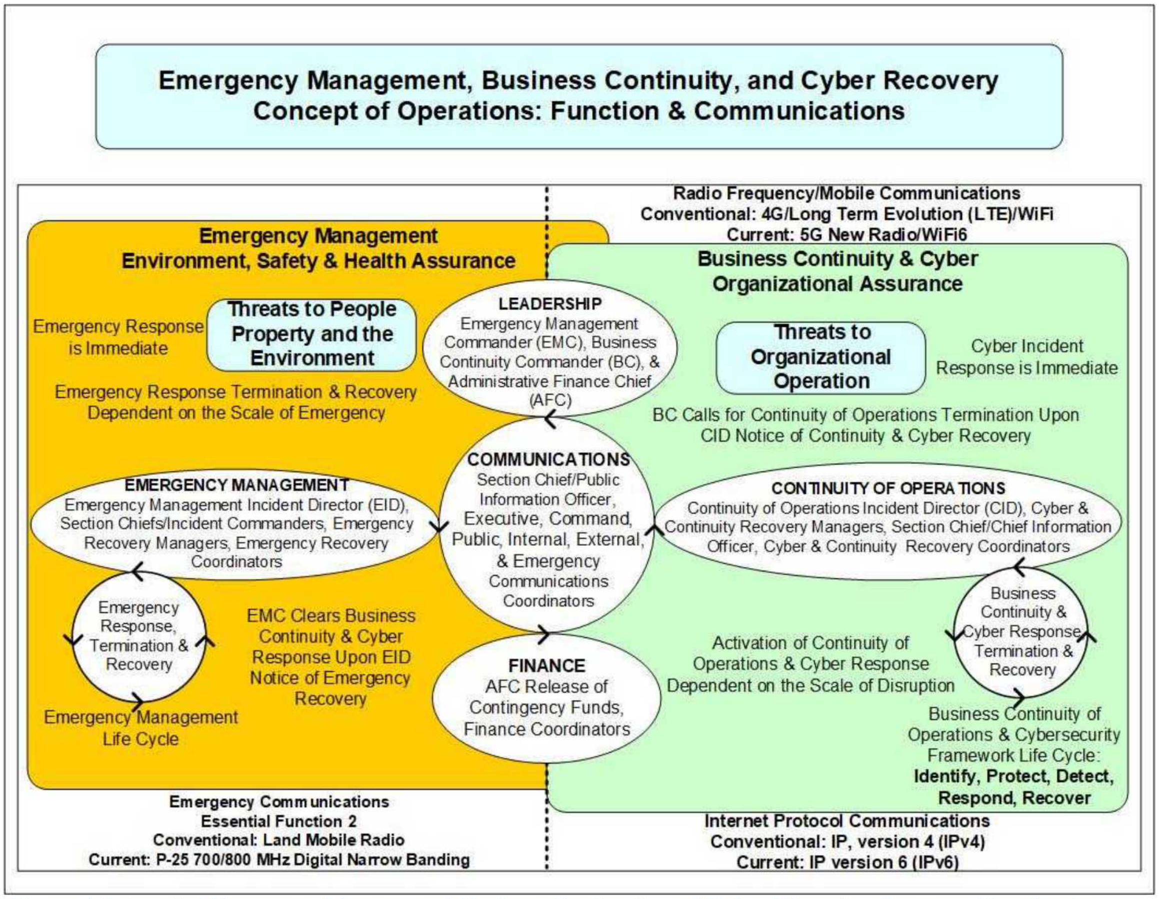

Emergency Management, Business Continuity, and Cyber Recovery
Concept of Operations: Function & Communications
Radio Frequency/Mobile Communications
Conventional: 4G/Long Term Evolution (LTE)/WiFi
Current: 5G New Radio/WiFi6
Emergency Management
Environment, Safety & Health Assurance
Business Continuity & Cyber
Organizational Assurance
Emergency Response is Immediate
Threats to People Property and the Environment
LEADERSHIP
Emergency Management Commander (EMC), Business Continuity Commander (BC), & Administrative Finance Chief (AFC)
Threats to Organizational Operation
Cyber Incident Response is Immediate
Emergency Response Termination & Recovery Dependent on the Scale of Emergency
BC Calls for Continuity of Operations Termination Upon CID Notice of Continuity & Cyber Recovery
COMMUNICATIONS
Section Chief/Public Information Officer, Executive, Command, Public, Internal, External, & Emergency Communications Coordinators
EMERGENCY MANAGEMENT
Emergency Management Incident Director (EID), Section Chiefs/Incident Commanders, Emergency Recovery Managers, Emergency Recovery Coordinators
CONTINUITY OF OPERATIONS
Continuity of Operations Incident Director (CID), Cyber & Continuity Recovery Managers, Section Chief/Chief Information Officer, Cyber & Continuity Recovery Coordinators
Emergency Response, Termination & Recovery
EMC Clears Business Continuity & Cyber Response Upon EID Notice of Emergency Recovery
FINANCE
AFC Release of Contingency Funds, Finance Coordinators
Activation of Continuity of Operations & Cyber Response Dependent on the Scale of Disruption
Business Continuity & Cyber Response Termination & Recovery
Emergency Management Life Cycle
Business Continuity of Operations & Cybersecurity Framework Life Cycle:
Identify, Protect, Detect, Respond, Recover
Emergency Communications
Essential Function 2
Conventional: Land Mobile Radio
Current: P-25 700/800 MHz Digital Narrow Banding
Internet Protocol Communications
Conventional: IP, version 4 (IPv4)
Current: IP version 6 (IPv6)

Figure 4. Integrated Emergency Management, Business Continuity, and Cyber Disruptive Response Coordination

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 continuity and cyber disruption response and recovery life cycles.

Conditions of Activation, Operation and Termination

Emergency operations have established methodologies for emergency response. 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). Business continuity, and cyber disruption response activation will work in-kind with Emergency management, meaning that the Emergency Management Commander has overriding authority over business continuity and cyber disruption response activation.

The Business Continuity Commander declares business continuity and cyber disruption response activation to initiate operational contingency plans that sustain critical processes and services. Section Chief's direct Coordination Officers and recovery teams through response to recovery operations. Contingency funds are concurrently released by the Administrative Finance Chief and communications are coordinated by the Public Information Officer. Contingency funds management includes cost recovery at the completion of recovery activities.

Contingency operations may run in conjunction with Emergency Management recovery operations through to completion of recovery as necessary. Recovery includes facilities, infrastructure, and services required to return to normal operations. Business continuity and cyber disruption recovery operations are not complete until consensus is reached from the Leadership Advisory.

Critical Considerations

Business continuity and cyber 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 of Critical Applications and Services
6. Identification of Critical Personnel
7. Identification of Critical Assets
8. Identification of Critical Processes
9. Identification of Vital Records
10. Staffing, Housing, and Alternate Work Sites
11. Established Command Structure
12. Managed Information and Communications
13. Prioritization of Activities
14. Training, Testing and Continual Improvement
15. Timely Implementation
16. Managed Legal Adjudication and Information Protection
17. Managed Contractual Obligations

Leadership Roles and Responsibilities

- 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 the leadership position that owns the responsibility for emergency management executive decisions and communications.
- Business Continuity Commander (BC) - The Business Continuity Commander is responsible for overall continuity and cyber coordination and communications. The Business Continuity Commander declares business continuity and cyber disruption response activation and termination in coordination with the Emergency Management Commander. The Business

Continuity Commander is the leadership position that owns the responsibility for business continuity and cyber disruption response executive decisions and communications.

- Administrative Finance Chief (AFC) – The Administrative Finance Chief is responsible for overall coordination of emergency contingency funding and cost collection. The Administrative Finance Chief is the leadership position that owns the responsibility for corporate financing.
- Section Chief – A Section Chief is responsible for coordination of area activities and reporting to the Emergency Management Commander and Business Continuity Commander any issues that require higher level attention. Section Chiefs may independently direct smaller, localized disruption response and recovery activities when necessary.
- Public Information Officer (PIO) – The Public Information Officer is responsible for consistent and accurate public relations and safety communications. The Public Information Officer is the leadership position that owns the responsibility for corporate communications.
- Leadership Advisory – 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.

Emergency Response Roles and Responsibilities

- Emergency Incident Director (EID) – The Emergency Incident Director is responsible for all emergency operations coordination and communications and may serve as the emergency management area Section Chief. The Emergency Incident Director is in place to coordinate multiple incidents 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. An Incident Commander/Section Chief may independently direct smaller, localized disruption response and recovery activities as necessary.
- Emergency Recovery Manager – Each Emergency Recovery Manager is responsible for coordination across the enterprise and collaborative business partners during emergency response activation. Emergency Recovery Managers report to the Emergency Management program office and coordinate closely with Emergency Recovery Coordinators. Emergency Recovery Managers ensure consistency in emergency response, safety, and application of resources across the organization.
- Emergency Coordination Officers – Each Emergency Coordination Officer is responsible for facilitating planning and training activities in times of order and provides coordination across a localized area during emergency disruption response, termination and recovery. Emergency Coordination Officer’s ensure consistency in safety and application of resources.
- Emergency Recovery Coordinator – An Emergency Recovery Coordinator is responsible for assisting Emergency Coordination Officers in support of response, termination, and recovery of emergency activities.
- Finance Coordinator - A Finance Coordinator is responsible for supporting Incident Commanders and Emergency Recovery Managers by facilitating financing for emergency response/recovery operations and facilitating cost recovery as necessary.

Continuity of Operations and Cyber Roles and Responsibilities

- Continuity of Operations Incident Director (CID) – The Continuity of Operations Incident Director is responsible for all Continuity of Operations and Cyber response and recovery coordination and communications. The Continuity of Operations Incident Director may serve as the Continuity of Operations section chief. The Continuity of Operations Incident Director is in place to coordinate multiple a wide area during large scale continuity events.
- Continuity Recovery Manager – A Continuity Recovery Manager is responsible for mission recovery coordination, which includes the restoration of support services needed to perform mission during continuity operations and full recovery to normal operations.
- Continuity Coordination Officers – Each Continuity 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 continuity and cyber disruption response activation. Continuity Coordination Officer's ensure consistency in deployment and application of resources across the organization.
- Cyber Recovery Manager – A Cyber Recovery Manager is responsible for cyber response and recovery coordination, which includes IT disaster recovery and the restoration of support services needed during cyber operations to full recovery of normal operations.
- Cyber Coordination Officers – Each Coordination Officer is responsible for facilitating planning and training activities in times of order and provides coordination across the enterprise during continuity and cyber disruption response activation. Cyber Coordination Officer's ensure consistency in deployment and application of resources across the organization.
- Continuity/Cyber Recovery Coordinator - A Recovery Coordinator is responsible for supporting the resumption and recovery of business continuity and cyber recovery elements.
- Finance Coordinator - A Finance Coordinator is responsible for supporting Continuity/Cyber Recovery Managers by facilitating financing for continuity and cyber response/recovery operations and facilitating cost recovery as necessary.
- Community of Interest Officer – Optionally, Community of Interest Officers are responsible for business partner and oversight communication of contractual obligations or other areas of concern.

In closing,

Cyber innovation will continue to evolve in the coming years. Automation is anticipated to improve critical safety and security systems. ICS/SCADA systems will become increasingly automated, computerized and connected. Human behavioral and complex system anomalistic analysis will continue to aide embedded threat mitigation capabilities. It then becomes essential to design-in cybersecurity, physical security, and resilient critical infrastructure protection to counter increasing human and technological threats.

The integration of emergency, continuity, and cyber practices will continue to increase as a combined set of response and recovery capabilities. This document intends to inform such fulsome response, termination, and recovery.

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-NA-0003525.