Pacific Northwest
NATIONAL LABORATORY

PNNL- 32686

Business Continuity, Cybersecurity, and Backup Control Center

Standards, References, and Recommendations
White Paper

March 2022

Scott R. Mix

U.S. DEPARTMENT OF
ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov**

1.0 Introduction

This whitepaper provides an overview of U.S. and international standards associated with business continuity and cybersecurity. It contains extracts from a report that addresses continuity of operations issues (including establishing and the secure operation of a primary and backup control center) for a mid- to large-sized electric power transmission organization (e.g., a transmission system operator [TSO]). The overview focuses on U.S. and international standards and references, and makes recommendations on business continuity and recovery actions.

2.0 Standards, Recommended Practices, and Regulations Review

This section provides an analysis of various international standards and other recommended practices in the areas of business continuity and information security. This section reviews and summarizes practices from the following organizations:

- International Standards Organization (ISO)
- International Electrotechnical Commission (IEC)
- International Telecommunications Union (ITU)
- International Society of Automation (ISA)
- ASIS International (formerly the American Society for Industrial Security)
- National Fire Protection Association (NFPA)
- North American Electric Reliability Corporation (NERC)
- U.S. National Institute of Standards and Technology (NIST)
- European Network of Transmission System Operators for Electricity (ENTSO-E)
- European Union Agency for Network and Information Security (ENISA)
- The Uptime Institute

2.1 International Standards

International standards are developed by a stakeholder group using a consensus process, with strict rules governing the development, commenting, balloting, and approval processes. International standards, by their nature, are intended to be applicable worldwide, and do not contain any country or regional-specific requirements or language.

Standards from six international standards groups were reviewed for this whitepaper. They are:

- **ISO**

  The International Standards Organization[1] (ISO) is an international, independent, non-governmental organization with 167 national standards bodies as its members. Working through over 804 technical committees and subcommittees, it brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards that support innovation and provide solutions to global challenges. Since its founding in 1946, ISO has published over 24209 international standards covering almost all aspects of technology and manufacturing[2].

- **ITU**

  The International Telecommunications Union[3] (ITU) is an agency of the United Nations specializing in information and communication technologies.

- **IEC**

  The International Electrotechnical Commission[4] (IEC) was founded in 1906, and is the world's leading organization for the preparation and publication of international standards for all electrical, electronic, and related technologies. According to their website, the IEC is one of three global sister organizations (IEC, ISO, ITU) that develop international standards for the world. When appropriate, IEC cooperates with ISO or ITU to ensure that international standards fit together seamlessly and complement each other. Joint committees ensure that international standards combine all relevant knowledge of experts working in related areas.[5]

- **ISA**

  The International Society of Automation[6] (ISA) develops standards and publishes books and technical articles, and conducts workshops, training, and certifications for automation systems and automation systems professionals.

- **ASIS**

  ASIS International[7] (formerly the American Society for Industrial Security) was founded in 1955 as an organization for security professionals that issues various certifications, standards, and guidelines for the security profession. It is accredited by the American National Standards Institute (ANSI) as a standards development organization.

- **NFPA**

  The National Fire Protection Association[8] (NFPA) was established in 1896, and is devoted to eliminating death, injury, property, and economic loss due to fire, electrical and related hazards.

[1] https://www.iso.org/home.html (accessed 11/05/2020)

[2] See https://www.iso.org/about-us.html(accessed 03/13/2022)

[3] https://www.itu.int/en/Pages/default.aspx (accessed 11/05/2020)

[4] http://www.iec.ch/ (accessed 11/05/2020)

[5] See https://tc114.us/about/about-the-iec/ (accessed 03/04/2022)

[6] https://www.isa.org/ (accessed 11/05/2020)

[7] https://www.asisonline.org/ (accessed 11/05/2020)

[8] https://www.nfpa.org/ (accessed 11/05/2020)

These organizations (and others) develop and publish international standards using a consensus development method in a variety of disciplines, including business continuity, physical security and cybersecurity. Some of the organizations (ISO, IEC, ITU) are primarily standards development organizations, while others (ISA, ASIS, NFPA) develop offer other services such as certification and training activities in addition to standards development. Many standards are co-developed and co-branded by multiple standards organizations (for example, ISA99 is also known as ISA/IEC 62443).

The international standards organizations copyright and sell their standards, so only a high-level summary of the standards is provided in this whitepaper. If additional detail is required, organizations will be required to purchase copies of the standards for review and reference.

2.1.1 ISO 22300

The ISO 22300 family of standards is part of the Societal Security family of standards, and addresses business continuity.

2.1.1.1 ISO 22301

Standard ISO 22301 describes a generic framework than an organization can use to establish a business-continuity management system. At a high level, business-continuity management involves:

- understanding an organization's key products or services and the activities required to deliver them;
- understanding restoration priorities and required resources;
- understanding the threats to the business activities, dependencies between them and to other organizations, and understanding the impacts of not resuming them;
- having tested arrangements (processes, agreements, etc.) to resume activities following an incident; and,
- reviewing and updating the arrangements to assure they will be effective when required.

The standard describes seven areas that must be considered during the development of business continuity plan. They are:

- Context – formally document and understand the organizations functions; identify the organization's risk appetite; understand legal and regulatory requirements and constraints; and determine the scope of required business continuity
- Leadership – secure and understand management's commitment to business continuity; develop a business continuity policy; and assign organizational roles and responsibilities
- Planning – address risk and opportunities; define business continuity objectives; and develop plans to achieve the objectives
- Support – determine resources required to execute the business continuity plan; assure that personnel performing business continuity tasks are trained and competent; assure that employees are aware of the business continuity policy and plans, and understand their roles; develop communication plans including what will be communicated and with whom to

communicate; and develop and maintain formal documentation for the business continuity plan, including actions taken when executing the plan

- Operation – plan, implement, and control processes to carry out business continuity requirements; perform a business impact analysis and a risk assessment; prioritize business functions for recovery activities; select a strategy to achieve business continuity objectives; establish resource requirements; establish and implement procedures, including incident response structures, warning and communication, business continuity, and recovery; and exercise and test the business continuity plan on a periodic basis
- Performance evaluation – monitor, measure, analyze, and evaluate the business continuity processes and plans; perform internal audits to assess the business continuity plan; and perform management reviews to assure the business continuity plan remains adequate and effective
- Improvement – update the business continuity plan in response to issues identified during periodic testing, auditing, or management review

It follows the "plan-do-check-act" framework to categorize the process. The "plan" component is composed of the context, leadership, planning, and support areas; the "do" component is the operation area; the "check" component is the evaluation area; and the "act" component is the improvement area.

2.1.1.2 ISO 22313

Standard ISO 22313 provides guidance on how to implement the framework described in ISO 22301 by providing recommendations and suggestions for each area of the framework.

2.1.1.3 ISO 22316

Standard ISO 22316 provides guidance on assessing an organization's resilience. It provides specific guidance in three major areas:

- Principles – including general principles and coordinated approach
- Attributes for organizational resilience – including general attributes; shared vision and clarity of purpose; understanding and influencing context; effective and empowered leadership; a culture supportive of organizational resilience; shared information and knowledge; availability of resources; development and coordination of management disciplines; supporting continual improvement; and ability to anticipate and manage change
- Evaluating the factors that contribute to resilience – including general factors; organizational requirements; monitoring and assessment; and reporting

2.1.1.4 ISO 22317

Standard ISO/TS 22317 provides guidance on establishing, implementing, and maintaining a business impact analysis process that can be used in support of the operation component of ISO 22301. It establishes a set of prerequisite tasks and resources, and provides guidance on how the analysis should be performed.

Prerequisite tasks and resources include:

- Establishing the business continuity context and scope
- Establishing the business continuity program roles, including roles and responsibilities; roles and competencies; business continuity program commitment, and business continuity program resources

The analysis process includes:

- Project planning and management
- Product and service prioritization
- Process prioritization
- Activity prioritization
- Analysis and consolidation
- Obtaining top management endorsement of results
- Business continuity strategy selection

The standard also recommends the business impact analysis process be monitored and reviewed on a periodic (typically annual) basis, or following an organizational change.

2.1.1.5 Other ISO/IEC 22300 Family Standards

The ISO 22300 family includes a number of standards that did not appear to be relevant to the project, and were therefore not reviewed. These standards provide guidance in the following areas:

- export interoperability for video surveillance;
- examination of existing available technologies;
- planning mass evacuations;
- supply chain continuity;
- planning for the involvement of spontaneous volunteers;
- incident response;
- public warning;
- color-coded alerts;
- capability assessment;
- monitoring facilities with identified hazards;
- implementing a community-based landslide early warning system;
- human aspects of business continuity;
- message structure for information exchange;
- establishing partnering arrangements; and,
- conducting exercises.

Additional standards in the ISO 22300 family are either withdrawn, or currently under development, and were not reviewed.

2.1.2 ISO/IEC 27000

The ISO/IEC 27000 family of standards is the information security component of the information technology family of standards. It is based on a set of standards originally developed in the United Kingdom as British Standard (BS) 7799.

2.1.2.1 ISO/IEC 27001 and ISO/IEC 27002

The core components of the family are standards ISO/IEC 27001 and ISO/IEC 27002. ISO/IEC 27001 provides a high-level overview of the seven elements of an information security management program. It then provides a high-level description of the security requirements, grouped as 14 security control objectives containing 35 major categories, and 114 high-level control areas (as of 2018). ISO/IEC 27002 provides additional implementation guidance details for each of the 114 high-level control statements described in ISO/IEC 27001 (with some areas having more than one implementation option).

The seven elements of an information security management system described in ISO/IEC 27001 are:

- Context of the Organization – including understanding the organization and its context; understanding the needs and expectations of interested parties; determining the scope of the information security management system; and information security management system
- Leadership – including leadership and commitment; policy; and organizational roles, responsibilities, and authorities
- Planning – including actions to address risks and opportunities (general; information security risk assessment; information security risk treatment); and information security objectives and planning to achieve them
- Support – including resources; competence; awareness; communication; and documented information
- Operation – including operational planning and control; information security risk assessment; and information security risk treatment
- Performance Evaluation – including monitoring, measurement, analysis, and evaluation; internal audit; and management review
- Improvement – including nomenclature and corrective action; and continual improvement

The 14 control objectives from ISO/IEC 27001 and IEC/ISO 27002 are:

- Information Security Policies – including management direction for information security
- Organization of Information Security – including internal organization, mobile devices, and teleworking
- Human Resource Security – including prior to employment, during employment, and termination and change of employment

- Asset Management – including responsibility for assets, information classification, and media handling
- Access Control – including business requirements of access control, user access management, user responsibilities, and system and application access control
- Cryptography – including cryptographic controls
- Physical and Environmental Security – including secure areas and equipment
- Operations Security – including operational procedures and responsibilities; protection from malware; backup; logging and monitoring; control of operational software; technical vulnerability management; and information systems audit considerations
- Communications Security – including network security management, and information transfer
- System Acquisitions, Development, and Maintenance – including security requirements of information systems; security in development and support processes; and test data
- Supplier Relationship – including information security in supplier relationships; and supplier service delivery management
- Information Security Incident Management – including management of information security incidents and improvements
- Information Security Aspects of Business Continuity Management – including information security continuity; and redundancies
- Compliance – including compliance with legal and contractual requirements, and information security reviews

2.1.2.2 ISO/IEC 27019

ISO/IEC 27019 augments the implementation guidance provided in ISO/IEC 27002 providing implementation guidance for controls specific to the energy utility industry by supplying 41 extensions to the implementation guidance found in ISO/IEC 27002, and extending ISO/IEC 27001 with three new control objectives and 14 new control statements with associated implementation guidance.

Most of these augmentations are specific to control systems, but some are directly applicable to an organization’s use of a supervisory control and data acquisition (SCADA) system or energy management system (EMS) for monitoring the electric transmission or distribution system.

ISO/IEC 27019 provides additional implementation guidance in the following control areas:

- Organization of Information Security – internal organization, and mobile devices and teleworking
- Human Resources Security – prior to employment, and during employment
- Asset Management – responsibility for assets, and information classification
- Access Control – business requirements of access control, user access management, user responsibilities, and system and application access control
- Cryptography – cryptographic controls
- Physical and Environmental Security – secure areas, equipment

- Operations Security – operational procedures and responsibilities; protection form malware; logging and monitoring; control of operational software; technical vulnerability management
- Communication Security – network security management
- System Acquisition, Development, and Maintenance – security requirements of information systems
- Supplier Relationships – information security in supplier relationships
- Information Security Incident Management – management of information security incidents and improvements
- Information Security Aspects of Business Continuity Management – redundancies
- Compliance – compliance with legal and contractual requirements, and information security reviews

ISO/IEC 27019 provides additional control statements in the following control areas:

- Organization of Information Security – internal organization
- Physical and Environmental Security – secure areas
- Communication Security – network security management
- System Acquisition, Development, and Maintenance – security in development and support processes
- Information security aspects of business-continuity management – redundancies

ISO/IEC 27019 provides additional control areas in the following control objectives:

- Physical and Environmental Security – security in premises of external parties
- Operations Security – legacy systems, and safety functions

2.1.2.3 ISO/IEC 27003

Standard ISO/IEC 27003 provides additional guidance on implementing an information security management system using the seven elements of an information security management program described in ISO/IEC 27001, by providing a required activity statement, explanation, guidance, and other information for each of the seven areas.

2.1.2.4 ISO/IEC 27004

Standard ISO/IEC 27004 provides guidance on how to measure the performance and effectiveness of an information security management system. It is specifically used to meet the “monitoring, measurement, analysis and evaluation” clause of ISO/IEC 27001. It provides a rationale, and describes the characteristics, types of measures, and processes for performing the evaluation. Annex B of the standard described 35 specific example measurements, mapped to the controls in ISO/IEC 27001.

2.1.2.5 ISO/IEC 27005

Standard ISO/IEC 27005 provides guidance on information security risk management. The most current versions of the standard predates revisions to ISO/IEC 27001 and 27002; there have been a number of attempts to update the standard, but the update attempts have failed, so the standard is a bit out of date. It also appears to have overlap with the ISO 31000 family of standards for risk management, although 27005 does not reference any standards in that family. The standard establishes the process as six activities (context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review), and within each activity describes inputs necessary, actions to complete the activity, guidance on how to complete the activity, and expected outcomes derived after performing the activity. The standard also includes a number of annexes providing examples and additional information on how to perform the risk assessment.

2.1.2.6 ISO/IEC 27009

Standard ISO/IEC 27009 is an introduction to the sector-specific applications of ISO/IEC 27001 and ISO/IEC 27002.

2.1.2.7 ISO/IEC 27010

Standard ISO/IEC 27010 provides guidance on information sharing between sectors and organizations. It provides augmented control statements or additional implementation guidance in the following control areas (some of which are modified in the current version of ISO/IEC 27001):

- Information Security Policies – management direction for information security
- Human Resource Security – prior to employment
- Asset Management – responsibility for assets, information classification, and information exchanges protection
- Cryptography – cryptographic controls
- Operations Security – protection from malware, logging and monitoring, and information systems audit considerations
- Communications Security – network security management
- Supplier Relationships – information security in supplier relationships
- Information Security Incident Management – management of information security incidents and improvements
- Information Security Aspects of Business Continuity Management – information security continuity
- Compliance – compliance with legal and contractual requirements

Standard ISO/IEC 27010 also provides a number of annexes with useful information on sharing sensitive information, establishing trusted information exchanges, the traffic light protocol for identifying the sensitivity of shared information, and models for organizing an information sharing community.

2.1.2.8 ISO/IEC 27014

Standard ISO/IEC 27014 provides guidance on governance of information security, providing high-level principles and processes for the governance of an information security program. It describes five principles:

1) establishing organization-wide information security,
2) adopting a risk-based approach,
3) setting the direction of investment decisions,
4) assuring conformance with internal and external requirements, and
5) fostering a security-positive attitude.

It then describes five processes to be implemented in support of the following five principles:

1) evaluate current and expected performance against current security objectives,
2) provide direction about changes needed in the information security program,
3) monitor progress toward achieving the improvements,
4) communicate information about information security between management and stakeholders, and
5) assure the processes are followed through the use of internal and external audits.

2.1.2.9 ISO/IEC 27017

Standard ISO/IEC 27017 (co-branded as ITU X.1631) provides guidance on applying the security controls of ISO/IEC 27001 and 27002 to cloud services. The standard augments the implementation guidance provided in ISO/IEC 27002 providing 38 extensions to the implementation guidance found in ISO/IEC 27002, and extending ISO/IEC 27001 with two new control objectives and four new control statements with associated implementation guidance in the following areas:

- Information Security Policies – management direction for information security
- Organization of Information Security – internal organization
- Human Resource Security – during employment
- Asset Management – responsibility for assets, information classification
- Access Control – business requirements for access control, user access management, system, and application access control
- Cryptography – cryptographic controls
- Operations Security – operational procedures and responsibilities; capacity management; backup; logging and monitoring; technical vulnerability management
- Communications Security – network security management

- System Acquisition, Development, and Maintenance – security requirements of information systems; security in development and support processes
- Supplier Relationships – information security in supplier relationships
- Information Security Incident Management – management of information security incidents and improvements
- Compliance – compliance with legal and contractual requirements, information security reviews

The standard also specifies additional control areas for:

- Organization of Information Security – relationship between cloud service customer and cloud service provider
- Access Control – access control of cloud service customer data in shared virtual environment

It specifies additional control statements in the following areas:

- Asset Management – responsibility for assets
- Operations Security – operational procedures and responsibilities
- Communications Security – network security management

2.1.2.10 ISO/IEC 27021

Standard ISO/IEC 27021 provides competency requirements for information security management system professionals. It describes basic knowledge and skill sets necessary to implement an information security management program. It describes a set of “business competencies” and a set of “information security competencies”, mapping the competence topics to specific security program elements from ISO/IEC 27001, and describing the expected outcome of applying the competence topic, knowledge required to support the competence topic, and skills required to perform the competence topic.

2.1.2.11 ISO/IEC 27031

Standard ISO/IEC 27031 provides guidance on information and communication technology readiness for business continuity. While not formally linked with the ISO 22300 family of standards, it follows the same “plan-do-check-act” structure of those standards. It provides guidance on preparing information and communications technology for use during a disruption that requires a business continuity plan to be invoked. It provides an overview of how information and communications technology (ICT) systems interact with and support business continuity processes and activities, focusing on the technical aspects of business continuity (infrastructure, equipment, software, data, etc.). It provides guidance on the following topics:

- establishing the response plan;
- developing the requirements and strategic options for the plan, considering all aspects of information technology;
- implementing the plan, including training, pre-deployment of technology, managing incident response, and developing documentation to assist in the execution of the plan during a disruption;

- monitoring and reviewing the plan, including testing and exercising the plan and staff responses; and,
- providing continual improvement of the plan by applying corrective actions and plan updates based on tests and exercises.

2.1.2.12 ISO/IEC 27032

Standard ISO/IEC 27032 provides guidelines for “cybersecurity”, mostly focused on internet or “cyberspace” security. It contains an introduction to internet and cyberspace security, a description of cyberspace stakeholders, a description of assets in cyberspace, a discussion of threats against the security of cyberspace, a discussion of roles of stakeholders in cyberspace, a discussion of cybersecurity controls, and discusses a framework for information sharing and coordination.

2.1.2.13 ISO/IEC 27033

Standard ISO/IEC 27033 is a six-part standard providing guidance on network security design and implementation.

Standard ISO/IEC 25033-1 provides an overview of the structure of standard. It provides a high-level discussion of network architecture and design, and network security planning and management. It provides guidance on identifying risks and security control associated with network operations, and provides an overview of supporting controls, modeled after those in ISO/IEC 27002 and ISO/IEC 27005. It provides guidelines for the design and implementation of network security, reference example network scenarios focusing on risk, design and control issues, and a list of “technology topics” that need to be considered. Annex A provides a mapping of the topics discussed in ISO/IEC 27033-1 with control objectives and control statements from ISO/IEC 27001 and ISO/IEC 27002. Annex B provides example documentation templates.

Standard ISO/IEC 25033-2 provides guidance for the design and implementation of network security, focusing on planning, designing, implementing, and documenting network security. Annex A provides a mapping of the topics discussed in ISO/IEC 27033-2 with control objectives and control statements from ISO/IEC 27001 and ISO/IEC 27002. Annex B provides example documentation templates. Annex C provides a mapping of ISO/IEC 27033-2 with the ITU-T X.805 framework.

Standard ISO/IEC 25033-3 provides guidance on threats, design techniques, and control issues associated with networking scenarios. It provides an overview of the process that can be used to address various threat scenarios, and then presents a number of threat scenarios and suggestions for overcoming the threats. The scenarios presented are:

- Internet access service for employees
- Business to Business services
- Business to Customer services
- Enhanced collaboration services
- Network segmentation

- Networking support for home and small business offices
- Mobile communication
- Networking support for traveling users
- Outsourced services

Annex A of the standard provides a sample Internet Use Policy; Annex B provides a catalog of threats.

Standard ISO/IEC 25033-4 provides guidance on securing communications between networks using security gateways. These networks can be within an organization, between different organizations, and between the organization and the general public. It provides an overview of the kinds of threats that network interconnection can present, discusses some security requirements that can be followed to overcome the threats, and provides a mapping between the discussed threats and requirements. It then provides a description of common security control techniques that can be used to secure communications between networks. The discussed controls are: state-less packet filtering; stateful packet inspection; application firewall; content filtering; and intrusion prevention and intrusion detection. These controls can be implemented on different security gateway components, including: switches; routers; application-level gateways; security appliances; and security monitors. The controls can be applied in a number of different architectures, including: packet filter firewall; dual-homed gateway; screened host; and screened subnet. The standard provides guidance on product and architecture selection.

Standard ISO/IEC 25033-5 provides guidance on securing communications across networks using virtual private networks (VPNs). The standard provides an overview of VPN technology, and security threats associated with VPNs. It then discusses the security requirements for VPN implementation, and a set of security controls that can meet the requirements. It provides guidance on the design and implementation of a VPN, and provides guidance on selecting VPN equipment.

Standard ISO/IEC 25033-6 provides guidance on securing wireless internet protocol (IP) network access. The standard provides an overview of wireless technology (including personal area networking like Bluetooth, wireless local area network (LAN) technology like Wi-Fi, and wireless metro-area networks like WiMAX), and discusses common security requirements across all technologies. It discusses security threats unique to wireless technology, including unauthorized access, packet sniffing, rogue access points, radio frequency jamming (denial of service), and session hijacking, among other threats. It then discusses security requirements that need to be met (which are generally required for both wired and wireless networks), and how the requirements specifically apply for wireless networks. A set of security controls, specifically tailored to wireless networks, is discussed, along with security design techniques.

2.1.2.14 ISO/IEC 27040

Standard ISO/IEC 27040 provides guidance on storage security. It introduces various storage technologies and architectures, and storage security risks. It addresses detailed supporting controls for various types and architectures of storage, and provides guidance for design and implementation of storage security. Annex A provides guidance on media sanitization (i.e., assuring that no information can be retrieved from the media) for a number of different storage technologies and applications. Annex B provides guidance on selecting appropriate storage security controls for the storage technologies and architectures described in the main body of the standard.

2.1.2.15 Other ISO/IEC 27000 Family Standards

The ISO/IEC 27000 family includes a number of standards that did not appear to be relevant to the project, and were therefore not reviewed. These standards provide guidance in the following areas:

- controls for telecommunications organizations;
- integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1[1];
- organizational economics;
- protecting personal identifiable information in public clouds;
- mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002;
- application security;
- security techniques for incident management;
- security techniques for supplier relationships;
- identification, collection, acquisition, and preservation of digital evidence;
- specifications for digital redaction;
- selection, deployment, and operations of intrusion detection and prevention systems;
- assuring sustainability and adequacy of incident investigative methods;
- the analysis and interpretation of digital evidence;
- incident investigation principles and processes;
- techniques for electronic discovery;
- expectations for organizations performing audit or certification functions for information security management systems;
- performing audits; and,
- performance of auditors.

Additional standards in the ISO/IEC 27000 family are either withdrawn, or currently under development, and were not reviewed.

2.1.3 IEC 62351

IEC 62351 describes the handling of security for IEC 60870-5 (SCADA communications), IEC 60870-6 (inter-control center communications protocol - ICCP), IEC 61850 (substation automation), IEC 61970 (common information model - CIM), and IEC 61968 (distribution system information model). It is primarily concerned with security communications, but includes sections on authentication of users and security architecture.

[1] ISO/IEC 20000-1 is the international standard for information technology service management (ITSM)

IEC 60870-5 is not widely used in the United States or Canada; rather most SCADA communications use DNP3 (standardized as Institute of Electrical and Electronics Engineers [IEEE] 1815) in either traditional (serial) mode, or in network (transmission control protocol [TCP]/IP) mode. Secure versions of the DNP3 protocol are available, using the Secure Authentication features of IEEE 1815 rather than IEC 62351, and the IEEE has approved a standard (IEEE Std. 1711.2 – Secure SCADA Communications Protocol [SSCP]) for securing serial protocols.

Use of IEC 62351 for securing ICCP in North America is limited;[1] most implementations opt for LAN-to-LAN (also called point-to-point, router-to-router, or site-to-site) encryption, often using Internet Protocol Security (IPSec), VPNs, or similar protocols to secure their communications. While IEC 62351 would be expected to be applicable to an organization for securing ICCP, the more common alternatives noted result in IEC 62351 having limited applicability.

Use of IEC 61850 for substation automation is prevalent in Europe, and growing in North America. IEC 62351 is the predominant method for securing IEC 61850 traffic worldwide.

2.1.4 ISA/IEC 62443

ISA/IEC 62443 was originally developed by the International Society for Automation (ISA) as ISA-99. It is the international standard for securing process automation systems, primarily those found in manufacturing and process industries. In electric power, they have traditionally had the most applicability in power plant control, but its use and applicability are gaining adoption in other segments of the electric power industry. ISA/IEC 62443 is composed of at least 13 proposed or approved standards grouped in four areas: general, policy and procedure, system integrator, and component provider.

Since ISA/IEC 62443 is not directly concerned with control center systems or data communications, it may not be relevant to an organization’s control center communication.

2.1.5 ASIS SPC.1

ASIS SPC.1[2] was written prior to the development of ISO 22301 and covers similar topics. Its primary advantage is that it is available for download from the ASIS International website at no cost. A high-level comparison of it and various other business continuity standards is available from the SearchDisasterRecovery.com website[3].

[1] See Secure ICCP report available at https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26729.pdf (accessed 11/05/2020)

[2] Available at no cost from https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf (accessed 11/05/2020)

[3] See https://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/AcomparisonofASIS_BSIBCM01-2010withISO22301andPS-PrepStandards.pdf (accessed 11/05/2020)

2.1.6 NFPA 1600

NFPA 1600[1] also covers similar topics as ISO 22301, but there are a number of areas covered in one standard that are not covered in the other. NFPA 1600 provides additional specificity in a number of areas, and includes significant (more than 75% of the document) guidance to the standard. NFPA is more suited to mid-size and large organizations, while ISO 22301 is more flexible and suited to smaller organizations.

NFPA 1600 is also more likely required or implemented by U.S. organizations, while ISO 22301 is more likely implemented by non-U.S. organizations. Its major advantage is that, like ASIS SPC.1, it is available at no cost (for viewing, but not printing) from the NFPA website.

2.2 Industry and recommended practices

Industry and recommended practices are developed by a variety of processes, some including stakeholder input, others developed internal to their organization. The development process varies by organization, but is generally not as formal as that for an international standard (although some do follow that rigorous process). Industry practices generally apply to a specific industry segment or region, may contain country- or region-specific language, and are not intended to be applicable worldwide like international standards, but nonetheless contain many concepts that can be applied universally.

Industry and recommended practice documents are also generally available at no cost via the internet.

2.2.1 NIST

The U.S. National Institute for Standards and Technology[2] (NIST) publishes cybersecurity recommendations primarily for the U.S. federal government and its contract organizations. They are generally mandatory for U.S. federal agencies, and are often adopted by private industry. The NIST SP 800 (Special Publication 800) series documents include the NIST Risk Management Framework and Cyber Security recommendations. There are over 100 documents in the NIST SP 800 series covering a variety of security-related tasks, including risk management, incident response, security controls, and recommended practices. NIST SP 800 series documents (including final and draft versions) are freely available from the NIST website[3].

2.2.1.1 NIST SP 800-34

NIST SP 800-34, last updated in 2010, provides guidance for contingency planning for information systems. It focuses on contingency planning activities to recover from disruption of client/server systems, telecommunications systems, and mainframe systems. The guide can be used in support of the “contingency planning control” components of NIST SP 800-53, and provides guidance in support of the following types of plans:

[1] Available at no cost for viewing at https://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=1600&cookie%5Ftest=1 (accessed 11/05/2020)
[2] https://www.nist.gov/ (accessed 11/05/2020)
[3] https://csrc.nist.gov/publications/sp800 (accessed 03/04/2022)

- Business Continuity Plans,
- Continuity of Operations Plans,
- Crisis Communication Plans,
- Critical Infrastructure Protection Plans,
- Cyber Incident Response Plans,
- Disaster Recovery Plans,
- Information System Contingency Plans, and
- Occupant Emergency Plans.

2.2.1.2 NIST SP 800-53

NIST SP 800-53 documents control areas and control statements for cybersecurity of information systems (also referred to as information technology, or IT systems). The control statements are guidelines that are expected to be "tailored" for local use by an organization. Different control statements can be selected based on an impact assessment for the system being protected. Different baseline control sets can then be created based on the resultant impact level (high, moderate, low). Appendix D of NIST SP 800-53 provides the recommended starting point for developing these control baselines.

The latest draft version of NIST SP 800-53 (version 5, December 2020) is composed of control statements and guidance grouped into 20 areas, containing a total of 276 control statements, many with more specific control statement enhancements. Appendix I of the document contains a mapping of the NIST control statements to ISO/IEC 27001 control statements.

2.2.1.3 NIST SP 800-82

NIST SP 800-82 contains guidance for securing industrial control systems, – primarily for systems found in industrial processes, including power plants, and, to a lesser extent, transmission stations, and includes sections comparing industrial control systems (ICS) and IT systems, risk management and assessment, risk mitigations, and architecture considerations. It also contains a set of control statements and guidance modeled after those found in NIST SP 800-52, but applied to ICS. Unlike NIST SP 800-53, there are no specific control statements contained in NIST SP 800-82, but rather, recommendations and guidance on how to apply the control areas and control statements to an ICS environment. These recommendations and guidance also contain references to other NIST SP 800 series documents for further implementation guidance. Appendix G of NIST SP 800-53 contains an "ICS Overlay" for specific control statement tailoring applied to the controls in NIST SP 800-53 Revision 4, and provides additional ICS-specific implementation guidance for selected control statements.

SCADA/EMS systems are a combination of IT and ICS systems, so some recommendations from both standards may apply; however, the recommendations in SP 800-82 should take precedence. For example, SP 800-53 control AC-11 (Device Lock) would not be appropriate for a real-time control system such as a SCADA/EMS workstation, but control AC-3 (Access Enforcement) could be achieved in a SCADA/EMS even though it is not achievable in many ICS field devices.

2.2.2 NERC

The North American Electric Reliability Corporation[1] (NERC) has approximately 100 reliability standards covering operations, planning, cybersecurity, and personnel requirements for the "bulk electric system," or BES (i.e., the interstate transmission system and large generation). NERC standards are mandatory in North America (the lower 48 contiguous United States, the southern provinces of Canada, and the Baja-Norte region of Mexico). The remainder of Mexico may be connecting to the North American grid at some point in the future, and when interconnected, will become subject to the standards. Within the United States, compliance with the NERC standards is governed by the U.S. Federal Energy Regulatory Commission (FERC), and compliance is mandatory with sanctions and fines for non-compliance. In Canada, compliance is governed by individual provincial regulations. NERC and the NERC Regional Entities perform audits of organizations to assess their compliance with the standards, and recommend sanctions and fines in cases of non-compliance.

NERC standards are "performance standards"; that is, they describe what expected performance by an organization should be, but do not prescribe how to achieve the required outcomes. The standards themselves are composed of a set of requirements (the expected outcome), and a set of measures (used to assess whether the expected outcome has been achieved). Additional sections of the standards describe applicability, non-compliance levels, and in some cases, technical justification for the requirements. Some standards also contain optional guidance, but NERC is in the process of removing that from the standards document, and placing it in separate guidance documents. The implementation guidance describes one possible implementation, but not the only way to achieve compliance.

NERC's jurisdiction for establishing and auditing compliance with its standards is restricted to the BES consisting of the transmission system (e.g., transmission lines operating at greater than 100 kilo-volt) and large generation facilities (e.g., generating units with a name plate rating of more than 20 MVA)[2].

The most current version of the NERC standards is freely available from the NERC web site.[3]

2.2.2.1 NERC Critical Infrastructure Protection (CIP) Standards

This summary of the NERC CIP (Critical Infrastructure Protection) standards is taken from a previous PNNL report, *Recommended Guidelines for NERC CIP Compliance for Synchrophasor Systems*, PNNL-27062[4], and modified to be applicable to the context of an organization's Control Center systems. The summary is based on the version of the NERC CIP standards that was approved and in force as of November 2017. This section of the whitepaper has not been updated to reflect any development activities after that date.

[1] https://www.nerc.com/Pages/default.aspx (accessed 11/05/2020)

[2] The formal definition of what constitutes the Bulk Electric System is complex, and can be found in the *Glossary of Terms Used in NERC Reliability Standards* available at https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (accessed 11/05/2020)

[3] https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United States (accessed 11/05/2020)

[4] http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-27062.pdf (accessed 11/05/2020)

The NERC CIP standards cover cyber and physical security. They are organized as follows:

- CIP-002 – BES Cyber System Categorization
- CIP-003 – Security Management Controls
- CIP-004 – Personnel & Training
- CIP-005 – Electronic Security Perimeters
- CIP-006 – Physical Security Perimeters (surrounding BES Cyber Systems)
- CIP-007 – System Security Management
- CIP-008 – Incident Response and Response Planning
- CIP-009 – Recovery Plans for BES Cyber Systems
- CIP-010 – Configuration Change Management and Vulnerability Assessment
- CIP-011 – Information Protection
- CIP-012 – Communication Networking between Control Centers (under development)
- CIP-013 – Supply Chain (pending FERC approval)
- CIP-014 – Physical Security (of transmission stations and large Control Centers)

The NERC CIP Standards are composed of 43 Requirements (generally equivalent to control objectives), and 136 Requirement Parts (generally equivalent to ISO or NIST control statements), including all approved and proposed versions of the standards.

The NERC standards apply to Control Centers[1],[2], transmission stations, and generation plants. The categorization process in CIP-002 assigns impact levels of “high”, “medium”, or “low” to the reliability-based computer systems associated with the operation of the bulk electric system. The standards would likely apply to an organization’s Control Center and its SCADA/EMS system at a high impact, meaning that nearly all of the requirements would apply (a small number of requirements only apply to low-impact or medium-impact systems).

NERC CIP standards are intended to protect “BES Cyber Assets” (BCA) or “BES Cyber Systems” (BCS) At a Control Center, the BES Cyber System is the SCADA/EMS system, which is composed of individual components (servers, workstations, and networking equipment) that are considered BES Cyber Assets. (For purposes of this document, the terms “BES Cyber Assets” and “BES Cyber Systems” can be considered interchangeable.) In order to assure that the BES Cyber Assets are appropriately protected, the standards also apply to “Protected Cyber Assets” (PCA), which are other computers or equipment located on the same local area network as the BES Cyber Assets within the SCADA/EMS (i.e., within the electronic security perimeter), as well as the Electronic Access Control or Monitoring Systems – EACMS (e.g., firewalls, logging systems) and Physical Access Control Systems – PACS (e.g., key card systems, card readers, camera, physical logging).

[1] Note – in the context of the NERC CIP standards, the term Control Center has a specific formal definition. The capitalized term will be used to indicate the formally defined term.

[2] See the *Glossary of Terms Used in NERC Reliability Standards, op. cit.* for a complete list of NERC terms used in reliability standards.

CIP-002 – BES Cyber System Categorization

NERC Standard CIP-002 – BES Cyber System Categorization describes the method used to determine the “impact level” of a particular BES Cyber Asset or BES Cyber System, and applies to all organizations under NERC jurisdiction. It contains two requirements.

Requirement R1 specifies the process for determining the impact level of a BES Cyber System using criteria located in Attachment 1 of the standard. For an organization that only has a Control Center, the only BES Cyber System that meets the criteria is the SCADA/EMS at the Control Center, and it would most likely be classified as being high impact, making the SCADA/EMS at the Control Center a high-impact BES Cyber System. Note that the standard specifically includes the backup Control Center systems under the same criterion, so both the primary and backup SCADA/EMS systems at the primary Control Center as well as the SCADA/EMS systems at a backup Control Center are considered high impact.

If an organization does not have any BES Cyber Assets or BES Cyber Systems that meet the criteria, they must document their results (under Requirement R2), and do not have to comply with other CIP cybersecurity standards. This does not apply to transmission system SCADA/EMS Control Centers.

Requirement R2 specifies that the analysis process must be repeated annually, and the results approved by the CIP Senior Manager (see CIP-003 Requirement R3).

CIP-003 – Security Management Controls

NERC Standard CIP-003 – Security Management Controls addresses governance issues, and applies to organizations with BES Cyber Assets at all impact levels.

Requirement R1 specifies the topics for a set of required policy statements that is intended to apply generically to all high- and medium-impact BES Cyber Assets, and can be selectively applied to the policy requirement for low-impact BES Cyber Assets. There are nine required policy statement subject areas that must be included:

1. Personnel and training (CIP-004);
2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
3. Physical security of BES Cyber Systems (CIP-006);
4. System security management (CIP-007);
5. Incident reporting and response planning (CIP-008);
6. Recovery plans for BES Cyber Systems (CIP-009);
7. Configuration change management and vulnerability assessments (CIP- 010);
8. Information protection (CIP-011); and
9. Declaring and responding to CIP Exceptional Circumstances.

The first eight policy statements directly correlate to the remaining CIP cybersecurity standards (CIP-004 through CIP-011), while the ninth addresses a process for determining and declaring a “CIP Exceptional Circumstance” (e.g., a fire, or storm restoration) where strict compliance with a requirement cannot be completed without jeopardizing health or service restoration. The CIP

Exceptional Circumstance policy should describe the process for determining when and how it must be invoked, provide a documentation trail of when it was declared and when it ended, and the process for assuring that the intent of the CIP Standard's requirements were met after the event was over. The process should be consistent with a similar process for low impact, if one exists.

Policy documents are written at a high level, and are intended to be company-wide, or at least division-wide. Since most organizations will have a mixture of different impact levels, the standards allow that the policy statements can be written only for high- and medium-impact BES Cyber Assets (allowing low-impact policy statements, if they exist, to be stand-alone), or an integrated policy set for all impact levels can be written.

Requirement R2 contains the technical requirements for low-impact BES Cyber Systems, so it does not apply in this case.

Requirement R3 specifies that a CIP Senior Manager must be designated. The CIP Senior Manager is a corporate official (or equivalent) with authority to assure that the CIP Standards are being adequately applied to the BES Cyber Assets. The CIP Senior Manager is required to approve various actions and lists generated during the implementation of the CIP standards, in order to provide senior management oversight into the program, and to assure that attention is paid to implementing the CIP Standards at high levels in the organization, and assuring that appropriate resources are given to implementing the standards.

Requirement R4 specifies the creation of a delegation process that allows the CIP Senior Manager to designate some authority (generally approval of specific actions or reviews of required lists) to lower levels in the company. The only obligation that cannot be delegated is the annual approval of the policy documents from Requirement R1. A delegation process is not required, and if not used, a simple statement that "no delegations will be made" will suffice. If delegations are used, this process specifies the minimum expectations for the delegation process.

CIP-004 – Personnel and Training

NERC Standard CIP-004 – Personnel and Training addresses training and personnel issues, and applies to organizations with high and medium impact BES Cyber Assets.

Requirement R1 specifies the development of a security awareness program that must be refreshed at least once a calendar quarter (as compared with a similar program for low-impact BES Cyber Assets that must be refreshed at least once every 15 calendar months). This requirement only applies to users of the BES Cyber Assets, not PCAs, EACMS or PACS. This is an awareness program, so no formal attendance records are required. The intent of a quarterly refresh is to keep the security awareness program "fresh" in employee's minds. A common approach is to hang different posters in locations frequented by employees (e.g., break rooms, hallways), and on a quarterly basis, rotate the posters so that there is a visual change (color, shape, etc.) which causes employees to notice something different, and take a moment to see what the change was. Other examples of awareness program materials include emails, and "security minutes" at tailgate or employee meetings (similar to "safety minute" presentations). Many organizations with a mixture of high- and medium-, as well as low-impact BES Cyber Assets, use a common program to reach all their employees, and follow the quarterly refresh cycle.

Requirement R2 specifies the development of a formal security training program. Completion of the training program is required prior to being granted unescorted physical access or electronic access to BES Cyber Systems, PCAs, EACMS, and PACS, and the training must be re-completed annually. The following specific topic areas that must be covered by the training program:

1. Cybersecurity policies;
2. Physical access controls;
3. Electronic access controls;
4. The visitor control program;
5. Handling of BES Cyber System Information and its storage;
6. Identification of a Cyber Security Incident and initial notifications in accordance with the incident response plan;
7. Recovery plans for BES Cyber Systems;
8. Response to Cyber Security Incidents; and
9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

The training program should be updated whenever significant technology or process changes (which are mentioned in the training program) are implemented. The annual refresher will assure that all required employees eventually trained on any modified material. Formal training attendance records are required; and, while not required, good training programs generally include quizzes to assure that the employees have reviewed and captured the material.

Requirement R3 specifics the development of a "personal risk assessment" – PRA (more commonly referred to as a background check) be performed prior to granting unescorted physical access or any electronic access to a BES Cyber Asset. The PRA includes an initial identity check, as well as a seven-year lookback criminal records check with specific details on the minimum records to be checked, specifies that the organization must develop a set of criteria that constitutes "passing" the PRA, assuring that vendors and contractors undergo a similar PRA process, and assuring that the PRA process (but not necessarily the identity verification) process is repeated at least once every seven years.

Requirement R4 specifies that the organization must have an "access management program" to manage all unescorted physical access, all electronic access, and all access to storage locations containing BES Cyber Systems Information (i.e., information about BES Cyber Systems that could be used to compromise their operation), whether the locations are physical or electronic. The access management program must include the process used by the organization to determine whether access by individuals is "needed." It also specifies that, once a calendar quarter, access is reviewed to assure it is authorized and an annual review is conducted to assure that authorizations are still valid.

Requirement R5 specifies actions to be taken to revoke access once it has been determined to be no longer needed by an individual. For "reassignments and transfers" (i.e., the individual is still an employee), access must be revoked on the calendar day following a determination that access is no longer required. Note that there is no specific timeframe associated with what constitutes "no longer needed." This allows organizations to make business decisions about when access is no longer “required.” For example, if an employee is transferred or promoted, there will be a period of training for the employee taking over the job. The specific time associated with this training will be heavily dependent on the job and the individual. Additionally, there may be infrequent periodic processing (e.g., year-end processing) that may occur long after the promotion or transfer. There may also be requirements for back-up of the task in the event that the new employee is unable to perform.

On the other hand, if the employee has been terminated for any reason (i.e., the employee is no longer an employee), access must be revoked as soon as possible, but no later than the end of the next calendar day. The standard specifically states that revocation of external remote access and physical access is sufficient to “revoke access” to the BES Cyber Assets in this timeframe, and allows for 30 days to clean up and revoke (or disable) individual accounts on BES Cyber Assets.

The requirement also specifies that when dealing with account revocation, passwords for shared accounts (e.g., “admin” or “root” accounts) must be changed within 30 days, but allows for an extension if there is an extenuating operation circumstance (e.g., heat wave resulting in high power demands, or a storm restoration) of 10 days following the conclusion of the extenuating circumstance.

CIP-005 – Electronic Security Perimeters

NERC Standard CIP-005 – Electronic Security Perimeters addresses electronic (or logical) border protection surrounding BES Cyber Assets and establishing an “Electronic Security Perimeter.” It applies to organizations with high- and medium-impact BES Cyber Assets. Standard CIP-005 only applies to BES Cyber Assets and PCAs (i.e., all the systems inside of an Electronic Security Perimeter – ESP). ESPs are not required around PACS, and the requirements in CIP-005 deal with establishing and configuring firewall EACMS, so the requirements (except for the inbound and outbound traffic filtering) do not apply to the firewall EACMS computers. (They should, however, be applied to EACMS computers inside the ESP that perform logging or authentication functions.)

Requirement R1 specifies that organizations establish and document an “Electronic Security Perimeter” – ESP surrounding all networks to which BES Cyber Assets are connected using a routable protocol (e.g., TCP/IP). The requirement also specifies that inspection of data and traffic crossing the ESP must be performed, looking for malicious traffic, including malware, entering or exiting the ESP. Malicious traffic could include looking for unexpected protocols, unexpected command sequences, or unexpected code in the data stream.

Requirement R1 also specifies that all routable connections must pass through an Electronic Access Point – EAP, which is defined as a network interface on a firewall EACMS, and the routable communication passing through the EAP must be filtered in both inbound and outbound directions, with a documented reason for allowing the traffic, and a specific denial of all other traffic by default. This filtering is generally accomplished using a network firewall device, and the reason specified for allowing the traffic is often included in the firewall rule comments. There also needs to be a process or method for detecting known or suspected malicious inbound and outbound communication. This includes both connection requests and data flows on unexpected ports in either direction (generally performed by the filtering feature of the EACMS), and possibly unexpected data flows across authorized ports. Finally, authentication of dial-up connections must be performed.

Requirement R2 specifies that a process for managing interactive remote users must be implemented. In the context of the CIP standards, "remote" access is any access that originates from outside the ESP, regardless of "how far" outside the ESP. An "Intermediate System" (also known as a proxy server or a jump host) must be used to manage all interactive access coming from outside the ESP, The Intermediate System must not be located inside the ESP (it can be outside or "on" the ESP as part of the EACMS), since it is used to authenticate the interactive remote users. All Interactive Remote Access must pass through the Intermediate System and must use both encryption and multi-factor authentication that terminate on the Intermediate System. If the Intermediate System was inside the ESP, then unauthenticated and unauthorized interactive users would have access to the network inside the ESP, and could potentially have unauthorized interactions with the BES Cyber Assets prior to the authentication being performed. Communications that pass through the EAP into the ESP must be inspected for malicious traffic (see Requirement R1) prior to entering the ESP, but encrypted communications that terminate on Cyber Assets inside the ESP can't meet the inspection requirement.

Note that this requirement applies to "interactive" access, not "machine-to-machine" or "system-to-system" access. Interactive access refers to access initiated by a (human) user using a protocol that is typically associated with human interactions, such as *ad hoc* file transfer (e.g., ftp) or command-line access (e.g., telnet or secure shell – ssh). This has raised issues in cases where a management console automated process uses a traditionally interactive protocol (e.g., telnet) in order to perform its management functions. Since the firewall EACMS performing the filtering cannot determine from the protocol used or the command structures sent whether the commands are coming from an automated process in the management console, which would normally be thought of as a machine-to-machine interaction, these interactions should be passed through the Intermediate System. The management console should be programmed to perform the authentication as if it were coming from a human user.

The encryption obligation has placed some architecture restrictions on communication paths that require encrypted paths. For example, some network equipment located inside an ESP can only be managed using an ssh command stream, which is an inherently encrypted protocol. The solution proposed is to establish an ssh connection to the Intermediate System, decrypt and inspect the traffic on the Intermediate System, then re-encrypt it and send it through to the end device. This is allowed since the intermediate System is considered to be part of the EACMS, and the EACMS is where the traffic inspection needs to take place. From a security standpoint, if the traffic inspection and decryption are not done on the same computer, the two computers should be located in a demilitarized zone (DMZ) network, sometimes referred to as a perimeter network, to minimize traffic snooping and spoofing from unauthorized sources.

CIP-006 – Physical Security of BES Cyber Systems

NERC Standard CIP-006 – Physical Security of BES Cyber Assets addresses physically protecting BES Cyber Assets and establishing a "Physical Security Perimeter." It applies to organizations with high- and medium-impact BES Cyber Assets. Note that this standard does not apply to the physical security of the BPS elements themselves (e.g., lines, breakers, transformers), but rather to the BES Cyber Assets used to monitor and control them. In transmission substations, BES Cyber Assets are typically located in the control house inside the substation fence. However, in some cases, the BES Cyber Assets may be contained inside the BPS element cabinets (e.g., breaker control cabinets, transformer load tap changer cabinets), in which case CIP-006 requirements would also apply to those control cabinets containing the

BES Cyber Assets. In a Control Center, the BES Cyber Assets are typically located in data centers or control room operations theaters.

Requirement R1 requires the development of a security plan that contains the designation of a "Physical Security Perimeter" – PSP and at least one physical access control used to control unescorted physical access to only those personnel who have been granted unescorted physical access. It specifies that at least two different physical access controls are required. A keycard and pin or keycard and biometric are often used. It requires that procedures must be in place to monitor and alert for unauthorized access attempts to gain access to the PSP, or to access the Physical Access Control System. Logging is required for individual personnel access, including date and time of access. Logs must be maintained for at least 90 days to support after-the-fact investigations.

Requirement R1 specifies that cabling that exits a Physical Security Perimeter (PSP), but does not exit an Electronic Security Perimeter (e.g., cabling that runs from a data center PSP to a control room PSP but passes through the ceiling of an unsecured hallway) must be either physically or logically protected. Physical protection could be accomplished by encasing the cabling in conduit. Logical protection could be accomplished by encrypting the data prior to its exit from one PSP, and decrypting it after it enters the other PSP.

Requirement R2 specifies that a visitor control program must be implemented for anyone who enters the PSP, but has not been granted unescorted access to the PSP. The visitor control program should specify how employees manage visitors, including provisions for visitor hand-off from one escort to another escort, and observation of visitor behavior while in the PSP. Automatic or manual logging of all visitors is required, including time of initial entry and final exit for the day, and the point of contact (often the escort). Visitor logs are to be maintained for 90 days.

Requirement R3 specifies that a testing program must be developed and implemented to test all aspects of the Physical Access Control System, including card readers, door and window sensors, cameras, provisioning, and logging systems. All aspects of the PACS must be tested at least once every 24 calendar months, but this can be an on-going process that continually tests portions of the PACS, as long as each component test is within the testing period.

CIP-007 – Systems Security Management

NERC Standard CIP-007 – Systems Security Management addresses securing the BES Cyber Assets themselves, and applies to organizations with high- and medium-impact BES Cyber Assets.

Requirement R1 specifies that network and physical ports that are not used and that can be disabled, should be disabled. The language for logical ports allows for keeping an unused or unnecessary port enabled if there is no means of disabling the port (e.g., a firmware-based system that does not provide a configuration option to disable a logical port).

Requirement R1 also specifies that the unused physical input/output ports, such as network ports, console ports, universal serial bus (USB) ports, etc. must be protected against unauthorized use. This is often accomplished by physically disabling them by removing internal jumpers or installing port blocking locks in the ports to prevent them from being used. Disabling them via software (e.g., via configuration settings or by not starting software modules) is not recommended since the software or configuration could be compromised rendering the ports available for use.

Requirement R2 specifies that a security patch management program must be developed and implemented to assess each BES Cyber Asset (individually or by group or class) every month to determine if security patches applicable to the BES Cyber Asset's software configuration have been released. If so, within another month, either install the patch (to mitigate the vulnerability) or determine a vulnerability mitigation and document an action plan to implement the mitigation and eventually install the patch. Since BES Cyber Assets are real-time systems with limited capability to take them out of service to install patches, the mitigation and action plan allows the vulnerability to be temporarily addressed without installing the patch, decreasing the vulnerability until the patch can be installed. Due to operational concerns and maintenance schedules, patch installation could be deferred, in some cases, several years until an available maintenance window allow the BES Cyber Asset to be taken out of service for patch installation. The temporary mitigations will serve as a defense until the patch is installed, and can then be removed if desired (or left in-place as a defense-in-depth against future vulnerabilities).

Requirement R3 specifies that the organization must have in place a procedure to deter, detect, or prevent the introduction of malicious code onto the BES Cyber Assets, or into the BES Cyber System. If malicious code is detected, but not prevented from entering the BES Cyber Asset, the procedure must address how the malicious code's actions will be mitigated. Note that preventing the malicious code from entering or impacting the BES Cyber Assets is itself a form of mitigation. This is a case where the BES Cyber System concept can assist in mitigating or preventing the introduction of malicious code, if an individual BES Cyber Asset is incapable of detecting or mitigating the malicious code (e.g., a firmware-based BES Cyber Asset that cannot run anti-malware software). In this case, a border device (which could be an EACMS firewall or IDS) could detect or deter the code from entering the BES Cyber System, or it could mitigate an exfiltration attack by blocking malicious or suspicious outbound traffic. The requirements also specify that if the mitigation method is "signature based" (i.e., a traditional consumer-style anti-virus product), a process for updating and testing signature updates must be implemented.

Requirement R4 specifies that a process must be in place to generate, analyze, and respond to security events. At a minimum, successful and unsuccessful login attempts and malicious code detection must be logged. The process must include an analysis and escalation process for generating a response alert for an alert event that requires further response activities, and the procedure must generate a response alert in the event of a failure of the logging system. Logs must be kept for a minimum of 90 days to aid in after-the-fact investigations if technically feasible, and except for CIP Exceptional Circumstances.

Requirement R4, also specifies that at least every 15 calendar days, a review of logged events must be performed to assure that all significant and actionable events are being processed and appropriate alerts being generated.

Requirement R5 specifies that a process for enforcing authentication of interactive access is implemented. This is in addition to the requirement in CIP-005 for authorizing and authenticating interactive Remote Access, and applies to all local and remote interactive access (the CIP-005 process only authorized interactive "entry" into the ESP – the CIP-007 authenticates access to individual BES Cyber Assets).

Requirement R5 also specifies that an inventory of all known generic or default accounts be performed, and a list of individuals who have access to those shared accounts is maintained. All known default passwords must be changed.

Requirement R5 also specifies minimum password construction restrictions, and allows for implementing something less than the minimum if the BES Cyber Asset does not support the minimums (i.e., complex passwords cannot be used if the password character set is restricted to only numeric characters). If the minimum password construction requirements cannot be met, the organization must implement the maximum supported by the device, and demonstrate using vendor documentation the password construction supported. Passwords must be changed annually, with enforcement either technical (preferred) or procedural (if the device does not support a forced password change). A minimum number of password attempts before locking the account (permanently or temporarily) or generating a repeated failed access-attempt log event must be implemented.

Requirement R5 also specifies that unsuccessful login attempts be either monitored or managed by either locking the account after a number of unsuccessful attempts or generate an alert after a number of unsuccessful attempts. The standard is silent on the number of unsuccessful attempts to be used before locking or generating the alert, but five is generally considered to be a reasonable number, balancing the practicality of authorized users forgetting or mis-typing passwords against the security of a password being guessed by a brute-force attack. Similarly, the standard does not address how locked accounts can be unlocked. They can be unlocked manually by an administrator, or it may be possible to automatically unlock them after a sufficiently long time period, say 15 minutes to an hour, depending on the sensitivity of the BES Cyber Asset being protected, and the typical urgency of the need to access the BES Cyber Asset after the account has been inadvertently locked.

CIP-008 – Incident Reporting and Response Planning

NERC Standard CIP-008 – Incident Reporting and Response Planning addresses recognizing and responding to cybersecurity incident issues, and applies to organizations with high- and medium-impact BES Cyber Assets.

Requirement R1 specifies that the organization must have a procedure in place to identify, classify and respond to Cyber Security Incidents. This must include a process for determining whether the incident is a Reportable Cyber Security Incident, and if so, include the process for generating and submitting the report to the appropriate entity(s) (e.g., in the United States, the E-ISAC, DOE). The response procedures should include identification of roles and responsibilities of responders, and procedures for handling the incident (e.g., containment, eradication, recovery, resolution).

Requirement R2 specifies that the incident response procedures must be tested annually. The test can be response to an actual incident, a “paper drill” (or “tabletop”) exercise, or an “operational exercise.” The documented response plan and procedures from requirement R1 must be used in the test, and records of actions taken during the test must be maintained.

Requirement R3 specifies that lessons learned (if any) from the test must be documented, and of the lessons learned indicate that the procedure must be modified, the procedure must be updated within 90 days following the test, and the updated plan must be communicated to all persons with a role in the plan. Within 60 days of a change in responder roles or a technology (e.g., a replacement system from a different vendor) mentioned in the plan, the plan must be updated and communicated to all persons with a role in the plan.

CIP-009 – Recovery Plans for BES Cyber Systems

NERC Standard CIP-009 – Recovery Plans for BES Cyber Systems addresses procedures for returning BES Cyber Asset functionality following an incident that interrupts those functions, and applies to organizations with high- and medium-impact BES Cyber Assets.

The requirements in CIP-009 specify a parallel process to that in CIP-008, but for recovery following response actions in CIP-008.

Requirement R1 specifies that a recovery plan be developed, that includes specific conditions for activating the recovery plan and identifies roles and responsibilities for responders. It also requires that processes be implemented for backup and storage of all information needed to recover the BES Cyber Systems. This includes installation media for operating systems, installed products, applications, and data, as well as instructions on how to restore the system to a functioning state. For a firmware-based router, this could include firmware chips or equipment used to "flash" (install) updated firmware. The procedures must specify that a process be implemented for verifying that backups made for purposes of recovery or restoration will be usable when needed, and any verification failures are addressed. Backup failures could be either media failures, in which case, the backup media should be replaced, or procedural errors (e.g., not everything that should be backed up is included in the backup process). In the event of a process failure, the process must be updated, and the backup re-created. If the process has been in use for a period of time, and the failure is just noted, all previous backups should be examined to determine whether they are usable for recovery purposes, and if not, they should be marked so they are not inadvertently used for disaster recovery purposes. Finally, if the actions do not impede restoration to service, have procedures to preserve data for post-event analysis.

Requirement R2 specifies that the recovery plan be tested annually. The test can be response to an actual incident, a "paper drill" (or "tabletop") exercise, or an "operational exercise." The documented response plan and procedures from requirement R1 must be used in the test, and records of actions taken during the test must be maintained. The test should include a sample of all information that could be used in the recovery to assure that it is usable in the recovery process. Additionally, a full operational recovery test must be performed at least every three years.

Requirement R3 specifies that any lessons learned from the test be documented, and if the lessons learned indicate that the procedure must be modified, update the procedure within 90 days following the test, and communicate the updated plan to all persons with a role in the plan. Within 60 days of a change in responder roles, or a technology (e.g., a replacement system from a different vendor) mentioned in the plan, the plan must be updated and communicated to all persons with a role in the plan.

CIP-010 – Configuration Change Management and Vulnerability Assessments

NERC Standard CIP-010 – Configuration Change Management and Vulnerability Assessments addresses understanding what software and configurations are running on BES Cyber Assets and managing vulnerabilities on them, and applies to organizations with high- and medium-impact BES Cyber Assets.

Requirement R1 specifies that a software and configuration baseline be created and maintained for each BES Cyber Asset. The baseline includes software & operating system (including name, version, and patch level) or firmware (including version and patch level) as well as any customized software or configurations, and network accessible logical port configurations. Any deviations from the baseline for installed software must be authorized and documented. Undocumented deviations must be investigated, and if found to be legitimate, the baseline must be updated. For planned changes to the baseline, an assessment of the security controls from CIP-005 and CIP-007 must be performed and verified, and the baseline documentation updated after the change has been made.

Requirement R1 specifies that changes that affect the baseline must be tested in a test environment prior to be installed in the operational environment (or at least tested in a manner that minimized adverse effects to the operational system), with the test results being documented.

Requirement R2 specifies that monitoring for changes or deviations in the baseline must be performed on a monthly cycle, with a process to investigate any deviations from the baseline configuration.

Requirement R3 specifies that vulnerability assessments must be conducted annually. Vulnerability assessments may be automated scans (e.g., using a commercial tool), or may conducted manually via a tabletop exercise (e.g., gathering configuration and version information from the BES Cyber Asset, and reviewing vulnerability sites from NIST[1] or MITRE[2], and reviewing uninstalled patches to manually determine whether known vulnerabilities exist with the running configuration). The results of the vulnerability assessment must be documented, and a plan developed and implemented to address any vulnerabilities found.

Requirement R3 specifies that an active vulnerability assessment must be performed prior to adding a new Cyber Asset into the environment, unless it is a direct replacement or addition of an existing Cyber Asset with the same configuration. Any issues found in the assessment must be remediated before the new Cyber Asset can be installed into the environment.

Requirement R4 specifies that a plan for managing vulnerabilities from Transient Cyber Assets (e.g., computer test equipment) and Removable Media (e.g., USB memory) based on introduction of malicious code from those devices. The requirements are broken into three areas: 1) Transient Cyber Assets managed by the organization; 2) Transient Cyber Assets managed by third parties (e.g., vendors or contractors); and 3) Removable Media. Since there is greater control over mitigations that can be placed on Transient Cyber Assets managed by the organization, the requirements are more stringent and more straightforward. The specific performance expectations are:

[1] See the NIST National Vulnerability Database at https://nvd.nist.gov/ (accessed 11/01/2017)

[2] See the MITRE Common Vulnerabilities and Exposures Database at https://cve.mitre.org/ (accessed 11/01/2017) that is migrating to https://www.cve.org (accessed 03/04/2022)

1. For Transient Cyber Assets (TCA) managed by the organization:
   a. Manage the TCAs either in an ongoing basis by periodically scanning it and automatically applying antivirus and patch updates, or on-demand by scanning and patching it before each use
   b. Authorize the use of the TCA by users, locations, and uses
   c. Implement some form of software vulnerability mitigation, such as patch installation, read-only boot media, or system hardening
   d. Manage introduction of malicious code using antivirus software or application whitelisting, and
   e. Manage unauthorized use by restricting physical access to the TCA, utilizing full-disk encryption with authentication on the TCA, or use multi-factor authentication to access the TCA
2. For TCA managed by third parties:
   a. Review software vulnerability mitigation actions by the third-party, including installed patches, patching processes, and other software vulnerability mitigation actions
   b. Review procedures to prevent the introduction of malicious software, including reviews of antivirus software used, update level and procedures, read-only media, and system hardening procedures and actions
   c. Determine whether the reviewed actions are acceptable or require additional actions if not
3. For Removable Media:
   a. Authorize the use of the Removable Media by users and locations
   b. Mitigate malicious code on the Removable Media by scanning it before connecting it to the BES Cyber Asset

CIP-011 – Information Protection

NERC Standard CIP-011 – Information Protection addresses protecting information about BES Cyber Assets that could be used to compromise their functionality (such information is called BES Cyber Systems Information), and applies to organizations with high- and medium-impact BES Cyber Assets. BES Cyber Systems Information such as IP address and equipment model can be contained in configuration or data files extracted from the equipment.

Requirement R1 specifies that methods must be developed and implemented to identify information that meets the definition of BES Cyber System Information, and procedures for handling and protecting BES Cyber System Information, including marking of information and media containing BES Cyber System information, as well as procedures used during transit and storage must be developed and implemented.

Requirement R2 specifies that procedures must be in place to protect against the inadvertent release of BES Cyber Systems Information on storage media, by assuring that the information cannot be legibly retrieved from the media. If the media is to be reused inside of an ESP of the same or higher impact level, a simple erasure of the media may be performed. If the media will be reused outside of an ESP (e.g., used in a corporate environment), a more complete secure erasure may be used. If the media is to be disposed of, a more permanent erasure process, likely media destructions, is required. If whole-disk encryption has been used, destruction of the encryption key and a re-format is likely an acceptable information destruction process.

CIP-012 – Communication Networking between Control Centers (under development)

NERC Standard CIP-012 Communication Networking between Control Centers (under development) addresses protecting data that is exchanged between Control Centers (for example, between the primary and backup Control Centers, or between a Control Center and a Control Center of a business partner).

Requirement R1 specifies that a plan be developed and implemented to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.

CIP-013 – Supply Chain (pending FERC approval as of 2017)

NERC Standard CIP-013 – Supply Chain (pending regulatory approval) addresses mitigating risks that can be introduced in a supply chain.

Requirement R1 specifies that a supply chain risk management plan must be developed for use in planning and procurement of BES Cyber Assets that identifies and assesses cybersecurity risks from: i) procuring and installing vendor equipment and software, and ii) transitioning from one vendor to another. It specifies the following required elements of the plan:

1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cybersecurity risk to the Responsible Entity
2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cybersecurity risk to the Responsible Entity;
3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;
5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and
6. Coordination of controls for: i) vendor-initiated Interactive Remote Access, and ii) system-to-system remote access with a vendor(s).

Requirement R2 specifies that the plan from Requirement R1 must be implemented. However, "Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: 1) the actual terms and conditions of a procurement contract; and 2) vendor performance and adherence to a contract."

Requirement R3 specifies that the plan from Requirement R1 must be reviewed and approved by the CIP Senior Manager every year.

When creating the CIP-013 requirements, changes were also made to CIP-005 and CIP-010:

- **Standard CIP-005 Requirement R2** was changed to specify that a method for disabling remote vendor access (whether system-to-system or interactive) must be enabled.
- **Standard CIP-010 Requirement R1** was changed to specify that a method be implemented to assure the integrity and authenticity of any vendor-supplied software be performed prior to installation of the software.

CIP-014 – Physical Security (of transmission stations and large Control Centers)

NERC Standard CIP-014 – Physical Security (of transmission stations and large Control Centers) addresses the physical protection of electric transmission equipment and Control Centers.

Requirement R1 specifies that a risk assessment be performed for the electrical transmission equipment to determine which transmission stations require additional physical protections in order to prevent instability, uncontrolled separation, or cause cascading outages. The assessment must be performed at least once every 30 months, and must identify any Control Centers responsible for controlling equipment at the identified transmission station.

Requirement R2 specifies that the analysis be verified by an independent third party, which may make recommendations to change the results of the analysis.

Requirement R3 specifies that the operator of a primary Control Center identified in the analysis must be notified.

Requirement R4 specifies that the owner of an identified transmission station or Control Center must assess the specific threats and risks associated with each identified site.

Requirement R5 specifies that each owner of an identified transmission station or Control Center must develop and implement a physical security plan to address the threats and risks identified in the Requirement R4 analysis.

Requirement R6 specifies that each owner of an identified transmission station or Control Center must have an independent third party review the analysis from Requirement R4 and the plan from Requirement R5.

2.2.2.2 NERC Emergency Operations (EOP) Standards

NERC EOP (Emergency Operations) standards govern how organizations should respond to emergencies, including control center[1] failure.

EOP-008 – Backup Control Center Functionality

NERC Standard EOP-008 specifies what control center functions need to be backed up, requirements for formal documents specifying how the functions will be backed up, and a performance requirement for all functions to be restored within two hours.

[1] Note – the NERC formal definition does not currently apply to other NERC standards.

Requirement R1 specifies that an operating plan must be developed to assure that each entity can maintain its operations in the event of the loss of its primary control center. Restoration of functionality must be complete in two hours or less.

Requirement R2 specifies that a copy of the operating plan be available at the primary control center and the backup control center.

Requirement R3 specifies that Reliability Coordinators[1] must have a backup control center.

Requirement R4 specifies that Balancing Authorities and Transmission Operators must have backup functionality (either by having a backup control center, or by contracted services).

Requirement R5 specifies that the backup plan be reviewed and approved annually.

Requirement R6 specifies that the backup functionality not be dependent on another Reliability Coordinator, Transmission Operator or Balancing Authority.

Requirement R7 specifies that the operating plan be tested annually.

Requirement R8 specifies that the plan must be provided to the NERC region in the event that the primary control center was or is planned to be unavailable for more than six months.

EOP-011 – Emergency Operations

NERC Standard EOP-011 requires transmission operators and balancing authorities to develop emergency operations plans, specific to their functional role, and have them reviewed by their reliability coordinator, and update the plans to address any reliability gaps identified during the review.

Requirement R1 specifies that Transmission Operators must develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area.

Requirement R2 specifies that Balancing Authorities must develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate Capacity Emergencies and Energy Emergencies within its Balancing Authority Area.

Requirement R3 specifies that the Reliability Coordinator review the Operating Plan(s) to mitigate operating Emergencies submitted by a Transmission Operator or a Balancing Authority regarding any reliability risks that are identified between Operating Plans.

Requirement R4 specifies that each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator.

Requirement R5 specifies that each Reliability Coordinator that receives an Emergency notification from a Transmission Operator or Balancing Authority shall notify within 30 minutes,

[1] Organization terms used are from the NERC Functional Model – see https://www.nerc.com/pa/Stand/Pages/FunctionalModel.aspx (accessed 11/05/2020) for additional information

other Balancing Authorities and Transmission Operators in its Reliability Coordinator Area, and neighboring Reliability Coordinators.

Requirement R6 specifies that each Reliability Coordinator that has a Balancing Authority experiencing a potential or actual Energy Emergency within its Reliability Coordinator Area shall declare an Energy Emergency Alert, as detailed in Attachment 1 of the standard.

2.2.2.3 Security Considerations for High-Impact Control Centers

NERC's Critical Infrastructure Protection Committee (CIPC) is developing a guideline[1] to address design of high-impact control centers. This guideline discusses the following areas:

- Threat assessment – assessing the physical location and characteristics for the control center, including terrain and line-of-sight approaches, vehicle traffic as a potential attack vector, proximity to other potential targets (e.g., dense population, commercial districts, government offices), on-site potential targets (e.g., electrical assets, fuel storage), proximity response personnel, including company response, law enforcement, and emergency responders, assessment of historical events, and colocation of the control center with other company functions or tenants in a multi-tenant building.
- Security planning – including designation of a "zone system" composed of 5 zones:
  - a public zone including parking lots, and grounds surrounding the control center building, or internal concourses especially in a shared building;
  - a reception zone where public and facility staff meet, and where staff normally enter the building;
  - a support zone with limited access to facility staff and visitors for non-critical functions;
  - an operations zone with restricted access, continuous monitoring, and robust physical security for control room operations; and
  - a high security zone contained within the operations zone with more restricted access, used for computer equipment supporting the control room function.

    A matrix of security controls is provided, with implementation recommendations by zone.

  High-level details of the facility location and construction are also included in this section
- Security measures – discussion of measures that can be undertaken to reduce the threats, and reduce the impact of possible attacks, including development of security plans, designing the control center for resilience, credentialed security management professionals, and providing for change management and review of security procedures.

The guideline borrows from several other sources, including a NERC report to FERC on the implementation of NERC Standard CIP-014[2], the Canadian Government of Ontario IT Standard Number 25.18 Physical Security Requirements for Data Centres Version #1.2 dated 18 March 2015[3], the Royal Canadian Mounted Police G1-026 Guide to the Application of Physical

[1] The guideline is currently in unpublished draft form.

[2] See https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/CIP-014%20High%20Impact%20Control%20Center%20Report.pdf (accessed 11/05/2020)

[3] See https://files.ontario.ca/tbs-2019-11-14/go-its-25-18-data-centre-physical-security.pdf (accessed 11/05/2020)

Security Zones[1], Security Management in the North American Electricity Subsector: A Guideline[2], and NERC Standards CIP-004-6. CIP-006-6, and CIP-014-2.

2.2.3 ENTSO-E

The European Network of Transmission System Operators for Electricity[3] (ENTSO-E) does not publish specific public guidance for cybersecurity or business continuity. In July of 2017, ENTSO-E and the European Network for Cyber Security (ENCS) signed a memorandum of understanding to develop "state of the art cybersecurity regulation, practices & standards for the electricity transmission system." There do not appear to be any publicly announced products from this agreement.

ENTSO-E does, however, have operational requirements relating to "backup control room functionality" restoration and backup communication.

ENTSO-E Policy 6[4] describes availability requirements for data and voice telecommunications. Each control center is required to have two independent links from each control center to two other control centers, with each link required to have an availability of 99.9 percent including planned outages, with link speeds of a minimum of 2 Mbit/s. Operations voice communications are expected to be "high availability" and independent from public telephone systems, with backup voice communications mechanisms (e.g., public telephone or satellite communications) available.

ENTSO-E is also governed by the European Union's Network Code on Emergency and Restoration[5] that requires backup power supplies for voice communication for at least 24 hours. It also requires that each transmission system operator have at least one "geographically separate backup control room" with at least 24 hours of backup power. Additionally, the transmission system operator must have "an evacuation procedure for moving from the main control room to the backup control room, in a maximum time of three hours, including the operation of the system during the evacuation."

2.2.4 ENISA

The European Union Agency for Network and Information Security[6] (ENISA) provides recommendations on cybersecurity, supports policy development and its implementation, and collaborates with operational teams throughout Europe. ENISA publishes guidance document for cybersecurity, similar to the guidance documents published in the United States by NIST. ENISA currently has over 450 reports and other publications available[7] in more than 15 topical areas.

[1] See http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-026-eng.htm (accessed 11/05/2020)

[2] Unpublished – available from the E-ISAC at https://www.eisac.com (accessed 11/05/2020)

[3] https://www.entsoe.eu/ (accessed 11/05/2020)

[4] See https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/Policy_6_final.pdf (accessed 11/05/2020)

[5] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.312.01.0054.01.ENG&toc=OJ:L:2017:312:TOC (accessed 11/05/2020)

[6] https://www.enisa.europa.eu/ (accessed 11/05/2020)

[7] https://www.enisa.europa.eu/publications#c5=2008&c5=2018&c5=false&c2=publicationDate&reversed=on&b_start=0 (accessed 11/05/2020)

The following reports may be of interest:

- Communication network dependencies for ICS/SCADA Systems[1]
- Report on Cyber Security Information Sharing in the Energy Sector[2]
- Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors[3]
- Certification of Cyber Security skills of ICS/SCADA professionals[4]
- Can we learn from SCADA security incidents?[5]
- Protecting Industrial Control Systems. Recommendations for Europe and Member States[6]

While written from a European standpoint, the ENISA documents can nonetheless still provide useful guidance outside of Europe.

2.2.5 Uptime Institute

While not a standards organization, the Uptime Institute[7] publishes guidelines for high availability data centers, and certifies data centers based on their guidance. The Uptime Institute makes their guidance publicly available on their website[8].

The Uptime institute specifies four “tiers” for data centers, Tier I through Tier IV. Tier I describes a basic site infrastructure; Tier II describes a redundant site infrastructure; Tier III describes a concurrently maintainable site infrastructure, and Tier IV describes a fault tolerant site infrastructure.

3.0 Continuity of Operations Scenarios

Continuity of operations plans may be invoked by a large number of reasons, ranging from operational disruptions from computer hardware failures such as crashed disks, to building disruptions such as fire, to wide-spread natural or environmental disasters such as hurricanes. These disruptions and disasters can be broken down into groups based on the scale of the disaster and the disruption to The organization’s core business functions. Continuity of operations plans can be applied to both control room functions and non-control room functions.

[1] https://www.enisa.europa.eu/publications/ics-scada-dependencies (accessed 11/05/2020)

[2] https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector (accessed 11/05/2020)

[3] https://www.enisa.europa.eu/publications/maturity-levels (accessed 11/05/2020)

[4] https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals (accessed 11/05/2020)

[5] https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents (accessed 11/05/2020)

[6] https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states (accessed 11/05/2020)

[7] https://uptimeinstitute.com/ (accessed 11/05/2020)

[8] https://uptimeinstitute.com/resources/assets?filter%5Blanguage_id%5D=0&filter%5Bcategory_id%5D=1&filter%5Bpublished_on%5D=0&task=search&filter_order=a.published_on (accessed on 03/04/2022)

Many of the disruptions can be mitigated to some extent through design considerations or redundancies; however, in many cases, a disruption of larger magnitude than considered in the design or from an unexpected cause can overwhelm the design considerations and redundancies, leading to significant loss of one or more critical functions.

For example, the most likely cause of water damage is from plumbing overflows or burst pipes. Thus, water damage in a computer room can be largely mitigated by not locating restrooms, sinks, kitchens, etc. in areas above the computer rooms. However, other sources of water, such as roof leaks, cooling equipment leaks, water from adjacent restrooms, leaking water-based fire suppression, or even simple spills can still result in water damage to computer room equipment. Similarly, the impact of computer hardware failures can be mitigated through redundancy, but if the same disruption damages both sets of redundant hardware, or if a second disruption occurs before the first failed hardware system is repaired, may cause a loss of one or more critical functions.

Continuity of operations plans must consider all disruption and failure scenarios in order to allow the organization's core functions to continue. The plan should consider large and small disruptions, as well as short-term and long-term. Plans should be flexible so they can be adapted to different triggering events and different contingency scenarios. Small disruptions can turn into large ones, and short-term disruptions can extend for long periods of time. Plans should be developed based on the resulting impact to the organization's critical functions, not specifically the reason the plans are invoked.

For example, a plan that addresses continuing control room operations during and after a control room evacuation and relocation could be invoked for any reason that the control room needed to be evacuated, including fire, smoke, water damage, or weather. The plan would specify how to safely evacuate staff, and resume (or continue) real-time operations during the evacuation, and re-establish the control room functions in an alternate and safe environment. Recovery plans need to be a bit more specific, and may not be able to be completely developed ahead of the disruption. Even though the immediate continuity of operations is very similar, recovering from a fire in the control room or data center may be different than recovering from water damage.

Although there are different scenarios that would cause the continuity of operations plan to be invoked, in many cases, common responses can mitigate the impact of the disruption. For example, a procedure to allow non control room staff to telework from home could be used in the event of a fire or other physical damage to the control center building, a traffic or construction issue prohibiting staff from traveling to or accessing the control center site, or an epidemic that keeps staff from physically interacting with other staff in the control center.

There are numerous reasons to invoke a continuity of operations plan, including issues in the following areas:

- Information technology and control systems
- Internal to the control center building
- Control center site
- Access to control center site
- Weather and other natural disasters

- Civil and political unrest
- Terrorist attacks and sabotage
- Other

Each of these areas will be discussed in the following sections.

3.1 Information Technology & Control Systems

For information technology, the continuity of operations plan must be coordinated with the cybersecurity plan. Many disruptions can be prevented, or their impact minimized, by following cybersecurity best practices in system design and operational procedures. These practices can minimize the impact of hardware and software failures, as well as assist in containing the spread and impact of malware if it infects the information technology or control system computers.

Most control-room-based control system hardware and software failures are mitigated by having redundant primary and reserve computers, and multiple copies of stored data, but non-control room functions may not have redundant hardware or have real-time access to back-up data.

The most common causes of computer hardware failure are from failed disks and failed computer power supplies. Redundant hardware largely mitigates these failures, but relies on having the redundant hardware available to take over in the event of a failure. This is the case for control-room functions, but in the case of non-control room functions, the business continuity plan will need to be invoked. If the backup control center is configured either as a hot backup or for parallel operations, the non-control room functions could be similarly configured with redundant non-control room function hardware, allowing the non-control room functions to continue operations from the primary control center using computers and data resident at the backup control center, and using the high-speed telecommunications link between the two locations.

The impact of a single failed disk can be mitigated using RAID (redundant array of independent disks) technology that spreads data and recovery information across multiple disks. This technology provides for continued access to data following a single disk failure. Most RAID implementations allow for “hot swap” of failed disks (i.e., the failed disk can be removed, and a replacement inserted without requiring a power down or reboot of the disk controller), and an automatic re-build of the redundant data structures on the new disk. There are many different RAID technologies available[1], some focusing on data availability, and others focusing on increased performance, the most common being RAID-0 (maximum performance), RAID-1 (maximum availability, lowest storage efficiency), and RAID-5 or RAID-6 (compromise between speed and efficiency, allowing for one [RAID-5] or two [RAID-6] simultaneous drive failures without loss of data). RAID storage is often implemented using either network-attached storage (NAS) where the storage is located on the same computer networks used for computer communication, or using a storage area network (SAN) where the storage is located on a dedicated network optimized for storage access. Using either NAS or SAN storage allows a single storage system to be access by multiple computers. NAS and SAN systems are available with multiple controllers and network interfaces to reduce single points of failure.

[1] See https://www.snia.org/sites/default/files/SNIA_DDF_Technical_Position_v2.0.pdf (accessed 11/05/2020)

However, mitigations taken to protect data against hardware failures will not mitigate the impact of deleted files or data corruption by malicious software. The only mitigation to protect against data issues is a data backup program that maintains separate copies of the files and data. Traditional backup programs work well for backing up files, but specialized software is needed to assure a consistent backup of data in a database if the application needs to continue running while the data is being backed up. Traditionally, backups were stored on removable media such as magnetic tape, CD, DVD, or Blu-Ray disk, but the decreasing cost of magnetic disk storage has made using SAN or NAS attached storage an option. A combination of magnetic disk (for rapid recovery if needed) and removable media (for disaster recovery, or in the event that the NAS or SAN storage is unavailable) is recommended.

Software can also malfunction. Mitigations to malfunctioning software include testing using simulated and live data in a test environment, but not all data scenarios can be tested. Continuity of operations plans, in conjunction with software development and update procedures should require that, in the case of control room support systems, one of the primary / reserve computers be updated and tested using real data before updating the other copy of the software. This allows the new software to be tested while still providing an operational backup in the event that the update does not perform correctly. “Failing over” to the new system for testing, and “failing back” to the old version and restoring the old software on the updated computer if the test is unsuccessful, will restore working software functionality to both computers. For non-control room functions, capturing a complete backup of the old software before updating will allow the previous version of the software to be restored in the event that the updated software malfunctions. This can be accomplished in a number of ways, including creating a removable media (e.g., CD or DVD) copy similar to the backup created for disaster recovery; having multiple copies of the program on a traditional disk maintained either online during the test or removed from the computer; or using a separate test computer. These methods allow the previous software version to be restored if the new version does not properly work.

IT systems are also subject to corruption from malware such as viruses and ransomware. These corruptions can result in local computer issues, such as performance slowdowns or file deletions; exfiltration of sensitive information; or corruption of data. The cybersecurity plan and the continuity of operations plan should address multiple issues, including minimizing the spread of the malware, and multiple stages of recovery.

Minimizing the spread of the malware includes architecture and procedure decisions, including placing redundant primary / reserve computer systems on separate networks, and managing the movement of programs between the separate networks. Limiting access from control system networks to other networks, including business networks and the public internet will minimize the likelihood that malware will be introduced into the control system environment.

Continuity of operations plans should also consider the possibility of cybercrime like denial of service, virus hoax warnings, and ransomware, intentional or accidental loss of business records or data, and unauthorized disclosure of sensitive data. In some cases, like loss of data and ransomware, damage can be minimized by having backups and restoration procedures, but in other cases, like information disclosure, procedures to manage the event and minimize the damage may be all that can be done.

Continuity of operations plans should consider the possibility that malware is present on backups taken before the malware became active. For this reason, multiple copies of backups, taken at different times, should be maintained to minimize the impact of using a corrupted backup to recover from a malware-based operational disruption. For example, the PJM Interconnection (PJM), located in the Mid-Atlantic region of the United States, has implemented a parallel operations scenario with two control centers (PJM refers to them as AC1 and AC2) each with a primary / reserve main control system where either control center can fully operate the grid at any time. In addition to the four operational control systems, a “golden image” (GI) system and a “virtual backup control center” (vBUCC) system provide additional levels of backup in the event that all four control systems at both control centers are simultaneously compromised. There is not a lot of publicly available information about these backup systems or procedures, however, some information can be obtained from presentations given by PJM staff[1],[2],[3],[4] showing example timelines and configurations for these systems. PJM’s overall control center backup and performance information is openly available in *PJM Manual 01: Control Center and Data Exchange Requirements*[5].

3.2 Issues Internal to the Control Center Building

Continuity of operations plans are most associated with physical disruptions affecting either damage or access to physical spaces such as the control center building. The impact of some building disruptions can be mitigated (such as the previously mentioned water damage scenario), but others cannot. And, even though impacts can be mitigated, they cannot be eliminated entirely.

A common building disruption is related to a fire somewhere in the building. If the fire is located in the control room or data center, it has a direct impact on control room operations, and the continuity of operations plan must be invoked immediately to allow control room functions to continue with minimal interruption. If the fire is located in the data center, it will also affect non-control room functions.

If the fire is located in other parts of the building, for example, a fire in a kitchen or break room, local fire procedures will likely require a complete building evacuation, leaving the control room functions unattended until staff are allowed to re-enter the building unless special consideration are made for essential control room staff (for example, smoke mask emergency hoods and tanks of breathable air). Fire first responders may require building power be shut off while fighting the fire, resulting in a shutdown of the computers in the data center, possibly including the uninterruptible power supply (UPS) to the equipment. Even if the control room systems can run autonomously for a period of time, or minimal operations can be performed remotely (say from an evacuation rally point), the control system computers will be unavailable, and will stay available until power is restored and the systems brought up manually and checked for errors that may have resulted in the uncoordinated power shutdown. Even after the fire is put out, the

[1] https://www.nerc.com/pa/rrm/Resources/Monitoring_and_Situational_Awareness_Conference3/2%20Resilience%20Strategies%20Golden%20Image%20and%20Zonal%20State%20Estimation.pdf (accessed 11/05/2020)

[2] https://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/4.%20Event%20Response%20Strategies%20-%20PJM%20-%20John%20Baranowski.pdf (accessed 11/05/2020)

[3] https://www.nerc.com/pa/rrm/Resources/Monitoring_and_Situational_Awareness_Conference2/4%20PJM%20EMS%20Back-up%20Strategy_J%20Baranoski.pdf (accessed 11/05/2020)

[4] https://cred-c.org/sites/default/files/slides/2016_12-02_CREDC-Seminar-Series_Monken.pdf (accessed 11/05/2020)

[5] http://www.pjm.com/-/media/training/nerc-certifications/trans-exam-materials-2020/manuals-user-guides/control-center-and-data-exchange-requirements.ashx (accessed 03/04/2022)

staff may not be able to re-enter the building until it has been deemed safe (e.g., smoke cleared and the building inspected for structural integrity), or a fire investigation completed.

After the fire is put out, even if the fire did not affect the control room or data center, the building may be damaged to the point that access to the control room is blocked by fire damage, rendering it unavailable or unsafe to access. The control room or data center may have smoke or water damage resulting from a fire located near to, but not in, those areas. Smoke may also contain other hazardous or corrosive materials as a by-product of the fire. These chemicals may cause latent damage to computer equipment. Smoke and other combustion byproducts could have also entered the computers by way of cooling fans and air handling units resulting in potential damage to the computers themselves that may not be evident for some period of time.

Similarly, water used in fighting the fire whether from a sprinkler system or first responders, may have damaged the computers or rendered power cables unsafe to re-energize without verification and possible replacement. Water also can damage furniture and workspaces, including desks, consoles, chairs, carpeting, and structural elements such as walls, floors, and ceilings, making the control room workspace unusable until cleaned up or re-built.

Water fire suppression systems come in two major varieties – commonly referred to as “wet pipe” and “dry pipe”. Wet pipe systems maintain water supply in the sprinkler pipes at all times, and only need the sprinkler head to activate in order to put the fire out. Dry pipe systems (also known as pre-activation systems) need some sensor like a smoke detector or heat sensor to open a valve (pre-activate the system) to let water into the piping, but still require individual sprinkler heads to activate and release the water only where it is needed (the pre-activation step may also cut the power to the computers to minimize electrical hazards from the water). Wet pipe systems can develop leaks, which may cause water damage under wherever the leak occurs, while dry pipe systems do not have that problem. For this reason, most sprinkler systems in data centers are dry pipe systems.

Smoke and water may have also damaged hardcopy records and documents. Electronic versions of all hardcopy documents should be maintained with offsite backup copies to prevent loss during a cybersecurity or physical disruption scenario.

Similar damage from smoke and water could occur for non-control room and other business functions impacting both computer equipment and hard-copy records, as well as damage to furniture and workspaces.

Non-water fire suppression systems (e.g., FM200, Halon) can also cause room or building evacuations, and use of some may lead to equipment damage. In some cases, the fire suppression chemicals are released under pressure sufficient to dislodge ceiling tiles, and move lightweight furniture. Following any fire system discharge, after the fire is completely put out, the air in the rooms will need to be replaced with fresh air, and the equipment checked for damage from either movement or damage caused by the fire.

Internal water damage could also occur from other reasons, such as roof leaks, plumbing overflows, burst pipes, ground water seepage, or floods, especially if the control room or data centers are located partially or fully underground.

Water damage, if not properly cleaned up, could also lead to additional structural damage and mold growth causing unsafe building environments as well as equipment damage.

Hazardous materials and chemicals can also cause building evacuations. Common cleaning materials, such as chlorine bleach, ammonia, or other cleaning products can create hazardous chemicals when improperly stored or mixed together. Other commonly used chemicals, such as pesticides, can also lead to hazardous material incidents, if improperly used or stored. Hazardous materials may also be brought into the building intentionally, or enter through ventilation ducts from outside.

Natural events, such as earthquakes and hurricanes could result in long-term building damage resulting in the need to use the backup control center long after the natural disaster itself is over. If the building is physically damaged during the disaster, it may require significant reconstruction before it is safe to be used again.

3.3 Issues with the Control Center Site

In addition to disruptions inside of the control center building, there may be disruptions impacting the control center site that result in the invocation of the continuity of operations plans. While not necessarily requiring the building to be evacuated, heavy rain coupled with poor or blocked drainage may result in ponded water that impacts the ability to enter the building, or may lead to building area flooding. High winds may similarly result in debris such as trees or other materials on the building site blocking entryways, driveways, parking areas, or building access.

More serious issues, which may require site evacuation include hazardous materials such as fuel spill or natural gas leaks, can create an unsafe environment for staff or visitors. In some cases, a hazardous material spill on the site may require that the staff stay in the building and not evacuate until the spill can be cleaned up, in addition to preventing access to the site by additional staff or visitors.

External power, water, fuel, waste disposal, or other essential services could be disrupted resulting in the need to transfer control to the backup site for critical and essential functions. Loss of electric power is generally mitigated by the installation of a UPS with backup on-site generator, but the continuity of operations plan should consider actions that would be taken in the event that the UPS or backup generator does not perform as expected. For example, the UPS typically is connected to critical computer and lighting, but not air conditioning. The computers can typically run for short periods of time without air conditioning until the generator can be started. However, if the generator cannot be started, the computers will eventually need to be shut down to prevent damage from overheating, requiring operations to be transferred to the backup location.

If hot water is supplied by natural gas heaters, a natural gas supply disruption could lead to unsanitary conditions. If natural gas is supplied by onsite tanks (e.g., propane) a tank leak would require evacuation of the building and site to prevent unsafe conditions such as loss of life resulting from an explosion.

Water supply could also be contaminated (either by on-site or external contamination), making the external water supply unsafe for use by staff. Short-term water needs could be provided by an onsite water tank or bottled water, but that is a temporary solution, and only for potable water. Blocked sewage lines may lead to sewage backups (especially on lower floors) resulting in unpleasant and unsanitary conditions in the control center building. Blocked or improper storm drainage can result in standing water that may inhibit access similar to flood conditions.

Depending on the location, the storm water may enter the control center building leading to structural water damage, and environmental damage from mold and mildew in the same manner as water used to fight fires in the building.

While the control center should have the capability to continue operations for some period of time with limited non-critical functionality, prolonged disruption to power, fuels, or water should result in a building evacuation and relocation of critical functions to the backup location.

3.4 Issues with Access to Control Center Site

There may be conditions outside of the control center site that can cause the continuity of operations plan to be invoked. Excessive traffic, for example due to a celebration or parade, may make it difficult to access the site. Road construction may block common access roads, or cause excessive traffic on otherwise low traffic roads. In addition to construction, natural disasters may impact common traffic flows by creating road blockages, or damage to bridges and road overpasses, which could result in the inability for certain staff to commute to work, or significantly lengthen commute timeframes. Disruptions to public transportation, if available and used by employees, can also impact the ability of employees to report to work.

Hazardous material leaks, due to traffic accidents or natural disaster may also impact the ability to travel. Spilled materials on roads can lead to extended road closures while the materials are cleaned up, while ruptured tankers containing hazardous chemicals (e.g., chlorine gas) or fuels (e.g., gasoline), or natural gas pipeline leaks may result in wide-area (i.e., multiple road) closures due to hazardous conditions.

Fire or other disruption at adjacent or nearby locations may impact traffic during the emergency response or while post-emergency activities (e.g., cleanup) are being performed.

These conditions will impact staff reporting to work, as well as staff at work leaving to go home, and may impact the ability of emergency crews to respond to medical and fire emergencies at the control center site.

3.5 Weather, Natural Disasters, and Environmental Hazards

Weather and other natural disasters can be the most disruptive events that cause the invocation of a continuity of operations plan due to the potential amount of damage, and the breadth of impact they can have. A large hurricane can have an impact width of 170 km for wind and rain damage, impacting the control center site, roads, fuel supply, and telecommunications as well as staff and their families. Tornados, while having a smaller impact area, can cause significantly more damage from stronger winds. Electrical storms can damage electric power and telecommunications lines, damage computer equipment by electrical transients, and may cause fires.

Floods can impact buildings, as well as physical infrastructure, including power, telecommunications, and transportation. Flooding of the control center building can result in significant damage to the building and its contents, while flooding near the control center may impact the ability to access or leave the control center site. Flooding can also result in transportation disruption, either temporarily until the water recedes, or more permanently by damaging roads or bridges.

Earthquakes can result in physical damage and disruption to buildings and infrastructure, including underground infrastructure like buried power, telecommunications, or natural gas pipelines that are largely immune to damage from weather events and flooding.

Damage to both electrical and other critical infrastructure, such as telecommunications and fuel supply, can be expected for large-scale weather and natural disasters including hurricane, windstorms, rainstorms, and flooding, so even if the primary control center is relatively unaffected by the disaster, it may be unable to continue operations, requiring a relocation to the backup control center to continue operations.

Natural disasters can also induce panic resulting in mass evacuations clogging roadways, and overuse of telecommunications capabilities impacting both continued operations and critical function relocation activities.

Occurrence of most weather and natural disasters, such as hurricane, windstorms, rain, and floods, can be predicted, so business continuity plans can be invoked ahead of the disaster occurring. For a significant weather event, the backup control center should be activated ahead of the weather allowing the primary control center to be safely shut down and staff evacuated before the weather strikes, providing for a clean transfer of control with no interruption.

Other natural disasters, such as earthquakes, cannot be predicted in advance, so advance control center evacuation is not an option. Additionally, earthquake damage can be widespread resulting in significant problems for evacuation and relocation of critical functions.

Natural disasters can also lead to secondary effects. For example, an earthquake could rupture a natural gas pipeline; the leaking gas could explode leading to additional physical damage and fires.

Environmental contamination either on-site, near the site, or from some distance away, may lead to the need for evacuation or the inability to access the site completely. Leaking fuel oil storage on site may require cleanup, leading to temporary loss of access to locations on site during cleanup. Spilled chemicals from traffic accidents may result in cleanup actions long after the vehicles involved in the accident are removed. Fires may release contamination into the air, and even offsite fires may release contamination affecting any facility in the direction of the wind. Water remaining after putting out a fire may support the growth of mold and mildew. In addition to the immediate effects of the environmental disaster preventing use of the facility, long-term health impacts to staff may occur.

3.6 Civil and Political Unrest

Civil and political unrest and protests, even if not related to the organization, or near the control center site, can cause significant disruptions to pedestrian and automobile traffic due to crowds and police actions to contain the demonstrations. This may impact staff's ability to report to work, as well as the ability for emergency response personnel to respond to facilities, or the ability for staff to relocate due to an on-site disruption.

General strikes may result in transportation or other infrastructure outages that impact the organization's ability to continue operations. A general strike against telecommunications, for example, could result in disruption or damage to the telecommunications infrastructure resulting in a sudden loss of communications, or it could lead to deferred maintenance or lack of response to trouble calls resulting in degraded communications capability over time. Strikes can have indirect impacts as well. For example, strikes against other critical services could result in fuel disruptions and shortages, even if the strike is not targeted at fuel suppliers, or strikes against fuel suppliers could lead to outages in other critical infrastructures that rely on fuels to continue their operation or respond to disruptions.

Strikes and protests in other countries can impact the organization’s ability to continue operations as well. For example, a while a telecommunications interruption near the primary control center will impact overall operations, a similar telecommunications interruption in a different area or country may impact the ability to interact with the business partners in that country or area. Strikes or protests against key supply chain partners may impact the ability to maintain its systems, or obtain spare parts.

The organization should also consider the possibility of protests against themselves, for example, an environmental protest against the existence (or expansion) of a critical asset. Protestors could block all access to the control center site resulting in difficulties for staff to report to work or leave the site, prevent key vendors from entering the site to maintain systems or deliver fuel, or prevent (or at least hamper) first responders from responding for fire and medical emergencies. Protestors could also breach the control center site and cause significant damage to the site, staff vehicles, and the control center building, perhaps even breaching the building and causing internal damage to the building or staff.

Even a strike or protest against a building or site next to or near the control center could result in indirect blocked entrances and the possibility of physical damage to the control center site disrupting employees reporting to work.

Secondary impacts of protests may include the use of tear gas to break up protests (or potentially by the protesters themselves), which if used near the control center, may impact the air quality on the control enter site or in the building. Building air handling systems that can isolate internal air from the outside would mitigate the impact of this and other air-borne chemicals.

3.7 Terrorist Attacks and Sabotage

Terrorist attacks or sabotage can have similar impacts to facilities and functions as civil unrest if they are performed by an outsider or are not targeted specifically against the organization, by causing collateral damage to the organization’s facilities or disrupting access to the site. Terrorist attacks can lead to widespread panic, and general distrust of public places, like streets, and public transportation. Responses to terrorist attacks may lead to curfews and public transportation shutdown resulting in reduced ability to report to work, increased checkpoints for pedestrian or automobile traffic, and limited public gatherings.

A terrorist attack against the organization directly could be as simple as a telephoned bomb threat resulting in disruptions from evacuation and search to an actual attack against the organization’s facilities or computer systems. Although most terrorist and sabotage attacks are external, in some cases, they can be initiated by employees or other trusted insiders.

Sabotage against organization facilities, systems, or key suppliers can impact the organization as well. An insider could plant a computer virus on a critical computer system rendering it unusable, or destroying data. Similarly, an insider could physically damage computers records stored at the control center. Sabotage against a key supplier, such as a fuel supplier could result in the failure of that supplier to provide or deliver key supplies.

Workplace violence can have the same impact on staff as a terrorist attack, by impacting morale, absenteeism, creating fear, and increasing the turnover rate of staff, all resulting in a loss of staff productivity. It may also lead to workplace compensation, harassment claims, and the need for increased security procedures.

An attacker armed with a gun could breach the perimeter security, and create an active shooter scenario causing significant disruption and potential loss of life. Active shooter procedures and drills are common practice in U.S. organizations. Intruders could have the intent to hold control room operators hostage for ransom, or to force them to take specific operations.

Attacks initiated outside the facility could also have the intent to abduct or hold control room operators hostage for ransom, or to kidnap key personnel.

However, if the attacker is an insider (e.g., an employee or trusted visitor), the impacts can be significant. Attacks performed by an insider can target specific locations or functions within the organization that are not publicly known, and can be targeted to produce significant damage to facilities, technology, or stored information. While insiders are typically employees, trusted visitors like contractors, who have knowledge of processes, facilities, and building layouts, can use that knowledge to impact maximum damage. Anyone inside the control center building could cause a disruption by causing false fire alarms requiring evacuation and investigation. In extreme cases, insiders could intentionally start fires or plant explosives in the building to disrupt operations.

Incoming package inspection and vehicle searches are common mitigations against the introduction of bombs to the facility. Incoming mail should be inspected in a different building than the control center to minimize the impact on control room operations from an explosion during inspection.

Significant large-scale actions such as piracy and war cannot be discounted, although they are beyond the scope of this document.

3.8 Teleworking and Remote Access

As a result of the world-wide COVID-19 pandemic in 2020, many organizations have been forced to allow employee teleworking to maintain their operations. Even for companies that already allowed teleworking, the COVID-19 pandemic forced companies to implement teleworking on a scale not generally considered when teleworking technologies, policies, and procedures were initially developed. For organizations that had not considered teleworking, the pandemic required them to rapidly implement teleworking without sufficient time for well thought-out procedures or equipment purchases, resulting in over-utilization of remote networking resources (like corporate internet connections), lack of computer equipment in staff residences, and limited availability of information and resources typically found in office environments, such as hard-copy documentation and references. Remote teleworking is especially problematic for functions requiring access to specialized equipment or located in unconnected secure enclaves like control rooms.

The organization should create a corporate policy requiring all telework be performed on organization-owned and managed equipment. This will result an initial requirement to purchase additional computer equipment (i.e., laptops or tablets) for use by teleworking staff, but this expense can be offset by a multi-year plan to retire use of existing desktop computers, and replace all computer use with laptops or tablets equipped with docking stations retaining the use of existing external keyboards, mice, and monitors. Use of organization-owned and managed equipment will aid in assuring that the computer configurations are properly managed, only authorized software is loaded on the computers, and software is kept up to date (patched).

Teleworking equipment such as monitors, keyboards, mice, etc. can be either purchased for use by teleworkers in their houses if teleworking is expected to be permanently shared with in-office work, or in the case of extended teleworking with no definite return-to-office plans, equipment may be temporarily moved from the office to the telework location. Workspace limitations and workplace efficiency should be considered when determining the size of external monitors, and if multiple monitors should be used in the teleworking environment.

In order for teleworking staff to access corporate resources, remote access will need to be established between the teleworking locations and the corporate offices using encrypted VPN most likely using existing internet connections at the teleworking location and the corporate office (see VPN discussion below).

Teleworking staff will also need to have access to telephone, possibly including video telephone capabilities. If dedicated telephone sets are required, the VoIP telephone system can be extended to the teleworker’s location using the same VPN as is used for computer access. Alternatively, collaboration applications and services, such as Microsoft Teams, WebEx Teams, or Zoom, can allow teleworker computers to be used for voice and video communication. These applications can also be integrated with staff smartphones. Note that there are multiple versions of these applications and services, some with limitations and known cybersecurity vulnerabilities, so a thorough review of options should be performed before selecting specific product or version.

If teleworking staff will need to create or maintain hardcopy, printers should be provided at the teleworking location. Printers should not be network-connected (see VPN discussion below), but rather USB-connected to allow for access when connected to the organization’s network. The telecommuting policy should indicate how staff with printers will be reimbursed for supplies (e.g., paper and ink or toner) if they are not supplied directly by the organization. While not all staff will initially require printers, for extended telecommuting arrangements, most staff will eventually require printing something, so inexpensive ink jet printers may be appropriate for many staff, while small office / home office (SOHO) laser printers may be appropriate for other staff with intermediate volume printing needs. In some cases, access to high-speed large volume printers located in the organization’s offices may be necessary, for example when printing large reports or generating accounting invoices. Use of office-resident printers will require limited access to the office to retrieve printout.

As mentioned above, there may be time when limited visits to the office may be necessary to retrieve large volume output, retrieve reference material from offices, or perform certain tasks that require on-site access. If office visits will be allowed during extended teleworking during a pandemic, procedures should be established to limit the number of visits, the number of simultaneous staff visiting the office, and the length of time a visit can last. The procedure should clearly state what activities are permitted during an office visit (and certain activities that may be expressly prohibited), and who may authorize an office visit. A single person (with provision to delegate responsibility) for each physical location should be designated to schedule and monitor office visits to assure that a limited number of staff are in the office at a given time and to arbitrate requests for simultaneous access. The procedure may also consider whether multiple staff may visit at the same time if they are visiting different areas of the building; for example, one staff member in the control room and another retrieving information from the general office area. The procedure should also specify sign-in and sign-out procedures that minimize shared equipment (keyboards, pens) to minimize the spread of contagions. Additional procedures, such as temperature scans and health checklists may also be implemented.

In addition to reimbursement for printer supplies, the organization could consider offering a modest stipend to cover miscellaneous office supplies like pens, notepaper, binders, paper clips, etc.

Information security and cybersecurity will be important considerations for any teleworking environment, especially if extended beyond several days. Teleworking employees will need to have access to sensitive information, both computer-based and possibly hard copy, so secure storage (e.g., locked file cabinets) may need to be purchased for some teleworking staff. For staff that will be creating sensitive hardcopy documents (e.g., accounting or HR data), secure document disposal must be provided. Document shredders that create strips no more than 6 mm wide and 50 mm long (called cross-cut or micro-cut shredders) should be procured for staff who require access to hardcopy information. Inexpensive strip-cut shredders should not be allowed since the resulting paper strips can very easily be re-assembled to re-create the original documents. Policies and procedures should also be in place to limit the amount of hardcopy information produced by staff without appropriate document disposal equipment. For staff with little need for dedicated shredding equipment, an alternative is to securely store the documents to be shredded, and use office-resident shredders once returning to work. This could also be an option for large volumes of documents to be shredded by allowing staff to return to the office to shred documents.

3.8.1 Virtual Private Network Considerations

Most staff will need to connect to computers and services located at the office. In most cases, use of an encrypted VPN will be used. VPNs provide logical extensions of local network to telecommuting locations, so the teleworker's computer acts as if it is on the local office network. Most modern VPN implementations use the public internet as the mechanism to connect the teleworking location to the office, based on the assumption that most teleworkers already have broadband (e.g., moderate to high-speed) internet connections. These connections will be shared with other internet uses at the teleworking location, such as remote learning, entertainment, and other household members teleworking activities, so internet connection speed enhancements may be required for some staff.

The teleworking policy should clearly state whether the organization will reimburse staff for part or all of their internet connection.

VPN configurations can be implemented in essentially two configurations: "split tunnel" and "full tunnel". In full tunnel mode, all traffic from the telecommuter's laptop is routed across the VPN to the organization's control center site. As shown in Figure 3-1, traffic destined for the organization (shown by the black line) is processed through to servers in the organization's data centers, while any traffic not destined for the organization (shown by the red line) is sent back out to the target location using the organization's internet connection, as if the traffic was initiated within the organization's network. This configuration is more secure since all traffic to or from the teleworker laptop must pass through the organization's security screening and firewall. Any interactions from third-party sites must similarly pass through the organization's security screening and firewall. However, the organization's internet connections must process the traffic in both directions, once to or from the third-party site, and once to or from the teleworker's laptop so it needs to be provisioned to account for this increased traffic. (Note that in this mode, even access to the local network at the teleworker location will be routed through the organization's firewall, meaning that network-attached devices like printers at the teleworker's location cannot be directly accessed. This is the reason that USB-attached printers were recommended above.)

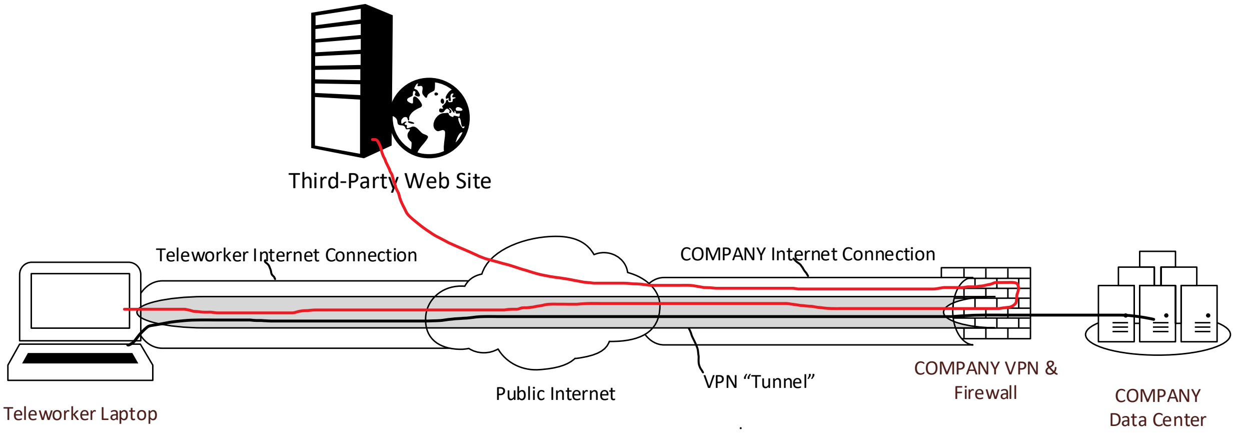

Figure 3-1: Full Tunnel VPN

In split tunnel mode, only traffic that is destined for the organization is sent through the VPN tunnel (shown by the black line), while traffic to other locations is sent directly to those sites (shown by the red line), as shown in Figure 3-2. This option is less secure since the organization's filtering and firewall will not see or filter any traffic between third-party websites and the teleworker's laptop. The benefit is that organization's internet connection will only need to process traffic that is destined for servers in the control center.

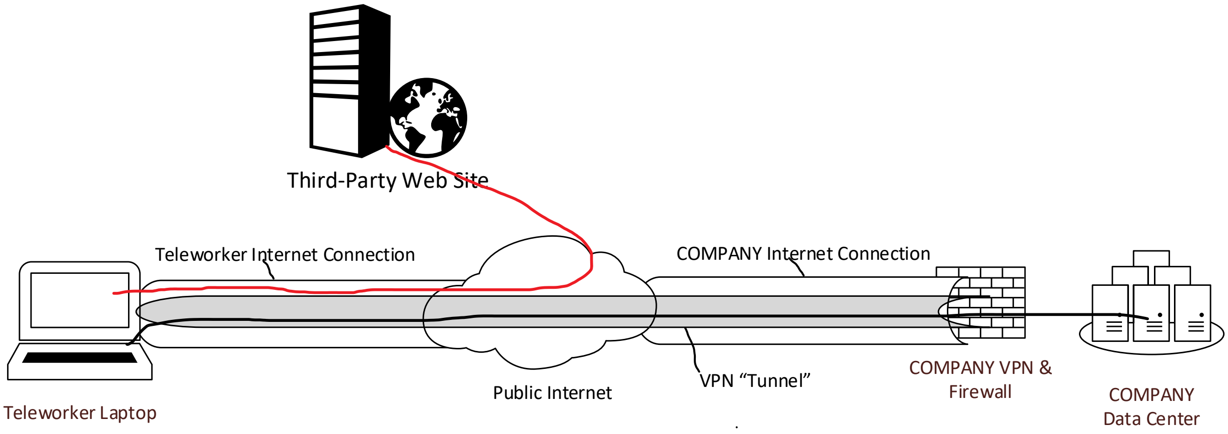

Figure 3-2: Split Tunnel VPN

In either case, the teleworker can access data and computer files in the data center as if they were connected to the internal networks, as long as the data is accessible from an internal network that is also accessible to the internet.

Split tunneling allows potentially malicious communications to take place outside the view of the organization's firewall, and if malicious code is installed on the teleworker's laptop, it could act as a router allowing the third-party website to have access to the organization's internal systems via the secured VPN connection, as shown by the orange line in Figure 3-3. If the teleworker has legitimate access to data being sent to the third-party website, there may be no alerts generated for the data loss, except possibly if the volume of data is higher than normal. Were this to be attempted using a full tunnel configuration, the VPN firewall at the control center would be aware of the data transfer, and could at a minimum, log it, or could block it as an unauthorized outbound access.

If the teleworker laptop had access to sensitive systems, the third-party website could just as easily issue commands to delete files or data inside the data center, or take other actions on systems that are behind the protection of the VPN firewall, since the teleworker laptop is logically "inside" the organization's network when connected to the VPN.

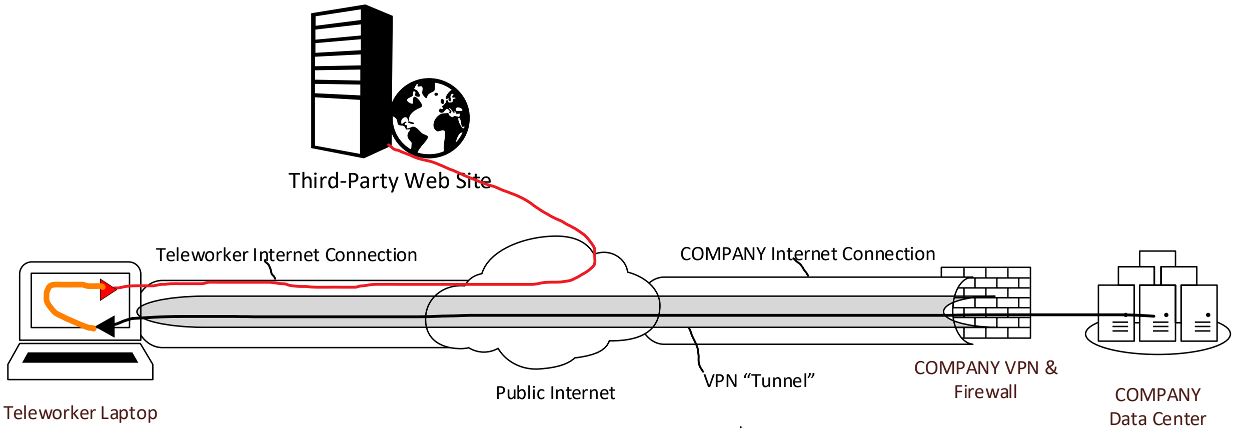

Figure 3-3: Data Exfiltration

In many cases, control room equipment, possibly including accounting systems, is isolated from the internet for security purposes, so a general-purpose VPN firewall will not be able to directly access those systems; an alternate architecture (with a separate VPN firewall and potentially separate internet connection) may be required. Use of this second connection should be restricted to only staff and functions that must access the secured equipment, and additional security, such as multifactor (at least two-factor) authentication and digital certificates may be appropriate to assure only authorized staff can access the connection.

Some VPN firewalls can be configured to allow access to specific systems or networks based on the authenticated VPN user. This could allow the same VPN firewall to be used by different general office users in different departments to only access specific systems. For example, staff with accounts assigned to the Human Resources department can be prevented from accessing Finance department systems and files. This will minimize access in the event that a teleworker laptop is compromised or maliciously used.

The VPN software itself can also be misconfigured or may contain vulnerabilities. Possible misconfigurations include use of split-tunnel when full tunnel is expected, allowing the end-user to change the configuration (e.g., change from full tunnel to split tunnel), change the encryption settings, or change the authentication mechanism. VPN software at both the client and control center end of the communication link may contain vulnerabilities, so constant monitoring for updates and installing security-related updates should be a high priority by IT staff.

Additionally, routine updates and software patches will need to be installed on teleworker laptops while they remain outside the orbitational perimeter. Update procedures (especially those for updating the VPN software) will need to work when connected to teleworker's home networks, and may require VPN connections to obtain the software updates – teleworkers should not rely on direct access to software updates from external sources or third-party websites, rather obtain them from organization-resident update servers. Procedures for performing updates should be developed, and the procedures automated as much as possible. The procedures should consider that if a computer reboot is required, with additional software installation after the reboot, the system will not be accessible until the teleworker reconnects to the VPN (this is especially important when updating the VPN client software since a failed upgrade will most likely render the laptop unable to access the organization's servers to correct the problem).

The update process should also specifically consider how anti-malware software and signatures are updated, even when not connected to the VPN, so that when the VPN connects, new signatures and associated scanning will not impede timely connection before the teleworker can connect to the organization and perform work.

Some VPN software can be configured to verify remote configurations before allowing the VPN connection to be established. Possible configuration checks include:

- Password presence and construction requirements
- Operating system and key application patch or update levels
- Presence of anti-malware software and signature levels
- Presence of unauthorized software

The VPN firewall itself must also be carefully configured and monitored. By its nature, it has access to the same sensitive networks and systems as the VPN clients will have once connected, so any compromise to the VPN firewall will allow a malicious actor to access those same systems. It could also be used as a launch point to access other systems on the same network even if VPN users don't normally require access to them. Constant monitoring for connections, performance, and configuration changes should be implemented to assure that no unusual or unexpected behavior can occur without initiating a response. Patches and updates for all software should be installed as soon as possible after release to reduce the likelihood of exploits against unpatched or out-of-date software.

Although dated, the following references provide background information on configuring and maintaining remote access to critical services:

- Initially published in 2003, the SANS Institute “Remote Access VPN – Security Concerns and Policy Enforcement”[1] whitepaper provides recommendations on setting up remote access connections.
- NERC released an industry advisory on “Remote Access Guidance”[2] in 2011 that made 10 recommendations for securing remote access, primarily for accessing control room equipment. It also referenced a separate NERC guideline “Guidance for Secure Interactive Remote Access” (now retired)[3] that provides implementation guidance based on practices implemented by organizations for providing secure access to control room equipment for both on-site and off-site remote access.
- In 2015 at their CIP Compliance Workshop, the Southwest Power Pool Regional Entity gave a presentation on NERC CIP Standards compliance issues with remote access called “Managing Interactive Remote Access”[4] that provides another set of recommended practices and configurations.
- The U.S. NIST Special Publication (SP) 800-53 Revision 5[5] “Security and Privacy Controls for Information Systems and Organizations” control AC-17 provides ten recommendations for remote access, and SP 800-46 Revision 2 “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security”[6] and SP 800-114 Revision 1 “User’s Guide to Telework and Bring Your Own Device (BYOD) Security”[7] also provide recommendations for remote access, including use of employee-owned computers for remote access.

A summary of the recommendations for remote access made in these documents is:

- Clearly define in corporate policy expected behaviors for staff when remotely accessing systems, and train staff on their expected behavior, including use of company resources for personal use, appropriate use of the equipment for internet access (i.e., only for authorized use), and who can use the teleworker’s computer (i.e., only the employee).
- Use dedicated company-owned equipment for remote access. This allows the equipment configurations to be controlled, including removing administrator access, removing unnecessary programs and configurations, configuration of a host-based firewall, controlled software installation and update, and management of anti-malware configurations.
- Use encrypted and securely authenticated access controls (i.e., a VPN) for remote access.
- Use a VPN termination firewall to process all internet connections for remote access. Consider adding or enabling intrusion detection and intrusion prevention capabilities on the VPN firewall.
- Use multi-factor (two or more factors) when authenticating remote users to the VPN firewall.

[1] See https://www.sans.org/reading-room/whitepapers/vpns/remote-access-vpn-security-concerns-policy-enforcement-881 (accessed 10/21/2020)

[2] See https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/2011%20Alerts/A-2011-08-24-1-Remote_Access_Guidance-Final.pdf (accessed 10/21/2020)

[3] See https://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf (accessed 10/21/2020)

[4] See https://spp.org/documents/29375/interactiveremoteaccessvideo.pdf (accessed 10/21/2020)

[5] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed 10/21/2020)

[6] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf (accessed 10/21/2020)

[7] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf (accessed 10/21/2020)

- Use different username and authentication methods on teleworker laptop, the VPN firewall, and internal systems. Use of one-time passwords (e.g., RSA SecureID® tokens or smart phone applications) may make remembering multiple passwords easier. This prevents compromise of one set of credentials from providing access to systems.
- Prohibit "VPN Split Tunneling" and network dual-homing[1] on systems used for remote access.
- Protect information about remote access mechanisms from unauthorized use and disclosure.
- Assure remote computers used to initiate remote access have current patches and updates installed and are running up-to-date anti-malware software. Some VPN clients provide for verifying patch levels and configuration settings and updating software prior to connecting to the VPN.
- Implement an inactivity timeout to automatically disconnect the remote access after a predefined period of inactivity. In some cases, the disconnection can be based on total connection time, rather than inactivity, to prevent background process communication from keeping the VPN connection active.
- As an alternative to providing remote access from general use remote computers, utilize a securely configured read-only boot device (such as a bootable CD or bootable read-only USB drive) to initiate remote access from non-company controlled remote computers.
- Implement logging and monitoring at the VPN access point for all user activity, including file transfers and program activation, as part of the VPN firewall server or with a specialized device for accountability.
- Implement an account lock-out feature such that an account is locked out for a period of time following a predetermined number of repetitive, unsuccessful login attempts.
- Perform periodic tests of the VPN configurations with unauthorized settings to assure that they are detected and prevented from connecting to the VPN.

If the organization is unable to supply teleworking equipment, processes described in NIST publications SP 800-46 and SP 800-114 for "Bring Your Own Devices" (BYOD) may need to be applied. Note that these processes can also be used to manage vendor- and contractor-owned equipment that is connected to the organization's networks whether remotely via VPN access or local direct connections to the organization's networks inside the control center.

3.8.2 Other Considerations

The organization should consider whether a "tiered" level of access can be used to support different access levels. For example, access to control room and accounting systems should only be performed on supplied remote equipment using strong multi-factor authentication with connection monitoring, while non-sensitive business functions may be able to use personal remote equipment with less stringent authentication requirements and limiting to what systems and information the remote users and devices have access. Access to email may be able to be accomplished on personal equipment including smart phones and laptops using web-based email clients. Access to collaboration sites, such as Microsoft Teams may also allow sharing of

[1] Dual-homing is when a single computer is simultaneously connected to two different networks. Normally, the computer does not route traffic between the two networks, however, network routing could be enabled by a careless or malicious user, or malware installation connecting the two networks. Dual homing typically uses two different physical network interfaces, but a split tunnel VPN configuration can implement dual homing with a single physical interface.

documents on smart phones and tablets if additional configuration protections are taken on those devices. Microsoft Teams could also be used to implement telephone connectivity for teleworkers allowing them to continue to use their office telephone number for in-bound and out-bound calls.

Secure web-based application portals such as CITRIX[1] may be used for read-only access to files or documents (such as production accounting results) if they are configured to use secure web access (using hypertext transport protocol – secured [HTTPS]), and include strong authentication mechanisms. While some application portals allow document modification, editing using the native portal applications can be problematic.

Application portals can also be used in “remote desktop” mode to allow remote access (either web-based or using a remote access client) to perform remote tasks on control center-resident computers. Application portals generally execute desktop applications on the application portal and provide screen and keyboard access to remote computers. These minimize the security risk of moving sensitive data to the teleworker location, but may require additional internet bandwidth to manage screen refresh, and the resulting screen views may not have the same resolution as native applications.

The organization should consider whether to restrict file upload and download when using the application portals to minimize the ability for malicious data infiltration (sending malicious data or programs to the organization) or data exfiltration (malicious retrieval of data from the organization) that could be performed by malicious code on the teleworker’s laptop. If file transfers are required, they could be restricted to only teleworkers that require the transfer.

Dedicated remote desktop applications and protocols such as Microsoft Windows Remote Desktop Protocol (RDP) may be used to provide remote access to Windows computers (as opposed to running applications) within the organization, such as the SCADA HMI screens or control center-resident desktop computers. If used, the organization should consider implementing a remote desktop gateway (RDP gateway) at the connection point between the corporate network and the SCADA system network to provide additional security. This configuration may allow use of a common internet access point for all VPN termination without significantly compromising connections to the SCADA system. The RDP gateway could also be used by non-teleworkers within the control center to access the SCADA system (likely to see view-only screens).

The RealVNC (virtual network computer) commercial remote desktop software[2] VNC® Connect provides remote desktop access for Windows and Linux workstations. The Professional subscription requires access via a cloud service meaning that all accessed computers need to have internet access in order to be accessed, and the access is achieved using internet (cloud) resident servers to facilitate the communication. The Enterprise subscription (at a higher cost) allows for direct connect (i.e., not using cloud services), and is more appropriate for access to SCADA systems. The VNC viewer client would connect to the organization via the secured and authenticated VPN, and then access the SCADA workstations from the corporate network through a firewall connection to the SCADA workstations. If this solution is implemented, the Enterprise solution is strongly recommended to minimize traffic exposure on external networks.

[1] See https://www.citrix.com/ (accessed 11/17/2020)

[2] See https://www.realvnc.com/en/ (accessed 11/18/2020)

Other remote desktop applications exist, but many contain identified security vulnerabilities and are therefore not recommended.

Remote desktop applications like RDP or VNC® Connect may be the only option for accessing specialized equipment like SCADA HMI screens.

In all cases, when accessing systems remotely from laptop or desktop computers, the access should use the secured and encrypted VPN to secure the access, even when using secured protocols like VNC® Connect or RDP.

Similar smart phone and tablet access could be provided after staff return to work using guest wireless connections (i.e., wireless connections at offices intended for visitor internet access that are not directly connected to internal networks).

Teleworking and remote access to systems also raise the issue of equipment loss and misuse beyond simple information theft. Theft or loss of remote laptop equipment containing sensitive information (including information and procedures used to access networks and systems) should be mitigated by protecting the computers from misuse following loss or theft. The organization should consider implementing whole-disk encryption, to minimize the ability to extract a disk from a lost or stolen laptop and accessing the information. Even though sensitive information may not be present on the laptop, it may have stored access information, including remote access applications, address information and cached credentials. Encrypting the disk renders the information unusable without the proper password.

The organization should also consider implementing boot passwords to prevent lost or stolen laptops from being used or information contained in them from being accessed. Whole disk encryption without using boot passwords allows access to the data on the disk if the laptop can be maliciously accessed through stolen logon credentials.

The organization should also consider whether remote lock and wipe software should be installed on laptops, tablets, or phones used by staff to access systems and data. When a device is reported stolen or lost, these applications will remotely lock and delete data when the devices re-connect to the internet. Many of them also include a locate function allowing the device to report its location (either network location or physical location if the device is equipped with a global positioning satellite receiver, such as found in a phone or tablet). Remote lock and wipe functions may be important to enable on phones and tablets with access to email to prevent information leakage from poorly protected email clients. In order to enable these functions on personal equipment, permission from the device owner may be required, and should be made as part of the conditions allowing email access on personal devices.

The organization should consider whether laptops that have been used for remote access for extended periods of time without being connected to the internal network should undergo an extensive scan for configuration changes, malware, and unauthorized program installation before being allowed to re-connect to the internal networks. While used for remote access, the VPN termination equipment and firewall have provided some level of protection against misconfigurations and unauthorized software, but those protections will not be in place once the equipment is reconnected to the internal network.

Teleworkers should also be aware of other forms information leakage, especially through home security system cameras and sound detection, smart appliances, digital personal assistants, and even baby monitors that may provide a mechanism to broadcast sensitive discussions to malicious listeners. Additionally, crowded households where remote learning and multiple teleworkers may simultaneously be broadcasting audio and video and inadvertently leaking sensitive information. Teleworking staff may find that in some cases, working from home may be as public as working from a coffee shop or internet café.

3.9 Other

Continuity of operations plans can also be invoked for non-traditional disruption scenarios.

Supply chain disruptions can impact the supply or delivery of critical supplies, and can be especially disruptive if the supplies are needed to repair broken equipment, or to replenish fuel. Supply chains could also be caused by political issues restricting shipment of equipment or spare parts across borders (either out of originating countries, or into final destination countries), by increases in tariffs, or by any of the issues previously discussed against the original manufacturer, the country of origin, or anywhere along the delivery path.

Supply chain issues could also require continuity of operations plans to be invoked to account for failed computer technology that cannot be repaired or is composed of obsolete hardware. Continuity of operations plans should consider how failed obsolete hardware and equipment can be functionally replaced. The organization should update their continuity of operations plan whenever new technology is installed to consider how the technology components would be replaced if needed, and it should review the replacement component list periodically to assure that the replacement plans are still valid. For example, if any critical functions are running on obsolete software platforms such as Microsoft Windows XP, replacement hardware may not be compatible with older versions of the software (e.g., new hardware without support for device drivers in Windows XP).

Lack of knowledge of how systems work, or how to repair them if they malfunction could also lead to loss of critical or essential functionality. This is especially true for internally developed software if the primary developer is unable or unwilling to repair software defects, or enhance the software for new functions in a timely manner.

A periodic review of deployed technology can identify equipment (hardware and software) that is nearing its end of life, or is approaching increased maintenance costs or activity due to its age. Planning and budgeting for replacement technology is significantly more cost effective than allowing the equipment or software “run to failure” to find out that it cannot be rapidly fixed or replaced.

Continuity of operations plans should also consider the impact to operations of incidents would not require a specific response, but may impact the ability for the organization to continue operations normally. Examples of this include theft and labor disputes. Procedures, coupled with strong policy and management commitment, can be put in place to detect theft of property or information from the organization minimizing the possibility of successful theft. Labor disputes by employees can be disruptive to operations, but would not necessarily require a relocation, rather an alternate staffing plan if, for example, the control room operators were to strike or refuse to work.

Employee morale should be considered while the continuity of operations plan is active. For the most part, employees can tolerate crowding and noise levels often found in temporary space for short periods of time – days to weeks, but if the temporary space is used longer, employee morale and work quality may suffer. The continuity of operations plan should consider both short-term and long-term relocation procedures to minimize this.

Public relations, including notifications to employees, families, business partners, government agencies, regulators, and the public should be part of any continuity of operations plans. Advance notifications that plans are in place in the event they are needed, as well as notification of tests and drills can provide regulators and business partners' confidence in the organization's ability to continue operations through a disruption. When invoked, notifications and press releases can be used to inform all affected parties of actions taken and the status of operations with the intent to maintain high levels of confidence that the organization is continuing operations in spite of the disruption.

4.0 Cybersecurity Plans

A proposed outline of the information and cybersecurity program document, based on the topics found in ISO 27001 and segmented with the additional topics from ISO 27019 follows below. The specific requirement statements and guidance can be extracted from the ISO standards, particularly ISO 27002 and ISO 27019, as well as other cybersecurity framework documents, such as NIST SP 800-82.

The outline represents a super-set of requirements that most U.S. electricity organizations implement based on their required compliance with the NERC CIP standards. U.S. federal power organizations (such as the Bonneville Power Administration or Tennessee Valley Authority) must follow the NERC CIP requirements as well as those specified by NIST in the SP 800-53 and SP 800-82 documents. U.S. electricity organizations are less likely to directly follow the ISO 27001 requirements for their control center systems due to the mandatory compliance with the NERC standards, but may follow them on a voluntary basis for their non-control systems.

The proposed outline represents a complete set of the requirement control areas from the ISO standards, some of which may not be directly applicable to the organization's current operation while some of them may over time become less important. For example, if the organization does not currently allow teleworking, but the continuity of operations plan will use teleworking as part of the continuity scenario, it should be addressed in the cybersecurity plan. Legacy equipment may be an issue with current systems, but even if the equipment is replaced with current generation hardware and software, at some point it will become legacy, and need to be addressed then, so those sections should be kept in the cybersecurity plan. Even if the organization has a procedure to maintain current versions, at some point it may not be possible to upgrade in a timely manner.

4.1 Suggested cybersecurity plan outline

1. Policy
    a. Policy set
    b. Policy review
2. Organization
    a. Internal organization
        i. Roles and Responsibilities
        ii. Segregation of duties
        iii. Contact with authorities

iv. Coordination with special interest groups
v. Information security in project management
vi. Risks associated with external parties
vii. Addressing security when dealing with customers

b. Mobile devices and teleworking
i. Mobile device policy
ii. Teleworking

3. Human resources security
   a. Prior to employment
   i. Screening
   ii. Terms and conditions of employment
   b. During employment
   i. Management responsibilities
   ii. Information security awareness and training
   iii. Acceptable use of the organization’s equipment and networks
   iv. Use of personal equipment to access the organizations systems or perform functions on behalf of the organization
   v. Disciplinary process
   c. Termination and change of employment
4. Asset management
   a. Responsibility for assets
   i. Asset inventory
   ii. Asset ownership
   iii. Acceptable use
   iv. Asset return
   b. Information classification
   i. Classification
   ii. Labeling
   iii. Asset handling
   c. Media handling
   i. Management of removable media
   ii. Disposal of media
   iii. Physical media transfer
5. Access Control
   a. Business requirements
   i. Access control policy
   ii. Access to networks and network services
   b. User access management
   i. User registration and de-registration
   ii. User access provisioning
   iii. Management of privileged access rights
   iv. Management of secret authentication for users
   v. Review of user rights
   vi. Removal or adjustment of access rights
   c. User Responsibilities
   i. Use of secret authentication information
   d. System and application access control
   i. Information access restriction
   ii. Secure log-on procedures
   iii. Password management system
   iv. Use of privileged utility programs

        v. Access control to program source code

6. Cryptography
    a. Cryptographic Controls
        i. Policy on use of cryptographic controls
        ii. Key management
7. Physical and environmental security
    a. Secure areas
        i. Physical security perimeter
        ii. Physical entry controls
        iii. Securing offices, rooms, and facilities
        iv. Protecting against external and environmental threats
        v. Working in secure areas
        vi. Delivery and loading areas
        vii. Securing control centers
        viii. Securing equipment rooms
        ix. Securing peripheral sites
    b. Equipment
        i. Equipment siting and protection
        ii. Supporting utilities
        iii. Cabling security
        iv. Equipment maintenance
        v. Removal of assets
        vi. Security of equipment and assets off premises
        vii. Secure disposal or reuse of equipment
        viii. Unattended user equipment
        ix. Clear desk and clear screens policy
    c. Security in premises of external parties
        i. Equipment sited on the premises of other energy utility organizations
        ii. Equipment sited on customer premises
        iii. Interconnected control and communications systems
8. Operations Security
    a. Operational procedures and responsibilities
        i. Documented operating procedures
        ii. Change management
        iii. Capacity management
        iv. Separation of development, testing and operational environment
    b. Protection from malware
        i. Controls against malware
    c. Backup
        i. Information backup
    d. Logging and monitoring
        i. Event logging
        ii. Protection of log information
        iii. Administrator and operator logs
        iv. Clock synchronization
    e. Control of operational software
        i. Installation of software on operational systems
    f. Technical vulnerability assessment
        i. Management of technical vulnerability assessment
        ii. Restrictions on software installation
    g. Information systems audit considerations

      i. Information systems audit controls
   h. Legacy Systems
      i. Treatment of legacy systems
   i. Safety functions
      i. Integrity and availability of safety functions
9. Communication security
   a. Network security management
      i. Network controls
      ii. Security of network services
      iii. Segregation in networks
      iv. Securing process control data communications
      v. Logical connection of external process control systems
   b. Information transfer
      i. Information transfer policies and procedures
      ii. Agreements on information transfer
      iii. Electronic messaging
      iv. Confidentiality of nondisclosure agreements
10. System acquisition, development, and maintenance
   a. Security requirements of information systems
      i. Information security requirements and analysis specifications
      ii. Securing application services on public networks
      iii. Protecting application services transactions
   b. Security in development and support procedures
      i. Secure development policy
      ii. System change control procedures
      iii. Technical review of applications after operating platform changes
      iv. Restrictions on changes to software packages
      v. Secure system engineering principles
      vi. Secure development environment
      vii. Outsourced development
      viii. System security testing
      ix. System acceptance testing
      x. Least functionality
   c. Test data
      i. Protection of test data
11. Supplier relationships
   a. Information security in supplier relationships
      i. Information security policy for supplier relationships
      ii. Addressing security within supplier agreements
      iii. Information and communications technology supply chain
   b. Supplier service delivery management
      i. Monitoring and review of supplier services
      ii. Managing changes to supplier services
12. Information Security incident management
   a. Management of information security incidents and improvements
      i. Responsibilities and procedures
      ii. Reporting information security events
      iii. Reporting information security weaknesses
      iv. Assessment of and decisions on information security events
      v. Response to information security incidents
      vi. Collection of evidence

13. Information security aspects of business continuity management
    a. Information security continuity
        i. Planning information security continuity
        ii. Implementing information security continuity
        iii. Verify, review and evaluate information security continuity
    b. Redundancies
        i. Availability of information processing facilities
        ii. Emergency communication
14. Compliance
    a. Compliance with legal and contractual requirements
        i. Identification of applicable legislation and contractual requirements
        ii. Intellectual property rights
        iii. Protection of records
        iv. Privacy and protection of personally identifiable information
        v. Regulation of cryptographic controls
    b. Information security reviews
        i. Independent review of information security
        ii. Compliance with security policies and standards
        iii. Technical compliance review

5.0 Continuity of Operations Plans

Continuity of operations plans focus on maintaining key critical and essential functions following a disruption or interruption to the normal processing associated with those functions. Creating a list of all functions performed by the organization, and assigning them a priority will aid in determining how the continuity of operations plans are developed. The continuity of operations plan focuses on the highest priority, or "absolutely must have" tasks as critical functions, with a primary emphasis placed on recovery and continuing any identified "critical real-time" functions performed in the control room, followed by other "critical" functions. Second priority is given to the "need to have" functions as "essential" functions.

When developing a continuity of operations plan, the ISO 22301 standards describes a process that can be used to develop the plan document and provides a high-level structure within which the plan should be developed. The ISO 22313 standard provides additional information about the subject areas that should be covered in the continuity of operation plan, but does not provide specific details about how those areas should be covered. It expects that an individual organization will provide the details following the development plan described in ISO 22301 and the subject areas contained in ISO 22313.

Following the guidance found in the ISO 22300 series standards, the continuity of operations plan should follow the Plan-Do-Check-Act (PDCA) model. The plan component includes creating policies, objectives, and procedures, and communicating them to staff. The do component consists of implementing and executing the plan by either testing it, or responding to an actual disruption. The check component includes monitoring the plan execution, and capturing lessons learned to improve the plan. The act component assures that the plan is improved based on lessons learned.

Continuity of operations plans should be developed and written at a high level in order to be flexible and general enough to be applied to numerous different scenarios. They should also be written to address "worst case scenarios" – it is much easier to scale back implementation of a plan than it is to try and expand it during a disruption. Staff experts may be unavailable to implement the plans during the disruption, so they should be sufficiently detailed to allow anyone with a general understanding of the technology to be able to implement them.

Most scenarios that require a continuity of operations plan to be invoked fall into one of a small number of general areas:

- Scenarios causing the temporary evacuation of the facility, such as a small fire in a non-critical area;
- Scenarios causing the long-term evacuation of the facility, and relocation of critical functions to other locations, such as a fire in the control room;
- Scenarios resulting from failed equipment – ranging from failure of one of a redundant pair of computers, to the failure of a non-redundant non-critical or critical component;
- Failures of external infrastructure, such as power, water, or telecommunications; and
- Scenarios involving the inability of staff to report to the work location, such as epidemic, weather disaster, or civil unrest not associated with operations.

5.1.1 Suggested Outline

Since the ISO 22300 standards do not specify the content of the continuity of operations plans, PNNL proposes the following outline for the continuity of operations plan document(s). The contents of ISO 22313 can provide a list of discussion items used to facilitate the development of more detailed plans to complete the continuity of operations plan, and can serve as a checklist to assure that all important areas are included in the plan.

1. Introduction
    a. Definitions
    b. Goals and objectives for continuity of operations
    c. Management commitment
        i. Assigning responsibility for creating and maintenance of continuity of operations plan
    d. Business Risk Assessment
        i. Selection of key business processes
    e. Scope
    f. Performance targets
        i. Critical functions
            1. Critical real-time control room functions
            2. Critical non-control room functions
        ii. Essential functions
        iii. Non-essential functions
    g. Description of functions to recover
    h. Continuity of operations assumptions
    i. Plan maintenance expectations

j. Plan review (every 6 or 12 months, and following significant changes)
k. Plan approval (and re-approval after review)
l. Plan posting and distribution
   i. Expectations for availability of plans (employees have a copy at work and one at home)
   ii. Can’t rely on electronic copy if the IT system hosting it is unavailable
   iii. Re-distribute after update

2. Preparation
   a. Continuity of operations priorities
   b. Incident Command structure
   c. Continuity and recovery procedures (details in appendices)
   d. Testing
      i. Tabletop
      ii. Simulation
      iii. Parallel
      iv. Full recovery
   e. Training
   f. Backup and offsite storage of critical data and records
   g. Prepositioning of equipment (critical control room and essential non-control room)
      i. Maintenance of prepositioned equipment – hardware, software, data
   h. Staff expectations and assignments
   i. Staff notification information (cell phone numbers for calls, texts, etc.)
   j. Supplies located at backup location
   k. Building evacuation plans and routes
      i. Rally points
      ii. Attendance procedures
   l. Staff relocation procedures
3. Pre-activation of incident response
   a. Used when the incident has warning, such as weather or scheduled protests
4. Initial incident response
   a. Informing Management of an incident
   b. Establishing the Incident command
   c. Declaring an incident
      i. Who can declare an incident?
   d. Response teams
      i. Responsibilities
      ii. Decision-making authorities
      iii. Assignments
      iv. Makeup, with designated backups
   e. Escalation procedures
      i. Thresholds
      ii. Events
      iii. Management involvement
   f. Communications
      i. Cell phone / text
      ii. Contact lists (cell phone, home landline phone, personal email)
      iii. Considerations if telephone / cell system unavailable
   g. Notification procedures
      i. Staff
      ii. Vendors

- iii. Business Partners
- iv. Regulators / Government
- v. Public

- h. Public Relations / Media
- i. Finance, Human Resources, Payroll
- j. Teleworking

5. Procedures for activating backup location
   - a. Business functions performed during relocation
     - i. Critical functions (e.g., control room operations)
     - ii. Essential functions (e.g., accounting)
   - b. Telecommunications – switchover / activation
   - c. Computer equipment – activation and validation
   - d. Data / records
     - i. Acquisition of data lost during activation and relocation
   - e. Critical staff relocation
     - i. Relocation routes – primary and alternate
     - ii. Relocation transportation
   - f. Essential staff relocation
     - i. Relocation routes – primary and alternate
     - ii. Relocation transportation
   - g. Non-essential staff functions
     - i. Short-term
     - ii. Long-term
   - h. Processing backlogged work
6. Re-establish primary location
   - a. Recovery teams
     - i. Responsibilities
     - ii. Decision-making authorities
     - iii. Assignments
     - iv. Makeup, with designated backups
   - b. Damage assessment
   - c. Restoration priorities
   - d. Salvage priorities
   - e. Insurance
   - f. Access to recovery information
     - i. Software installation
     - ii. Database backups
     - iii. Hard-copy records
   - g. Develop restoration / reconstruction plans
     - i. Building / structure
     - ii. Support systems (power, water, air handling)
     - iii. Furnishings (internal partitions, doors, windows, decorations, fixtures, furniture)
     - iv. Equipment (computers, printers, servers, copiers, networking, telephones)
     - v. Re-build IT systems
7. Procedures for returning to normal operations
   - a. De-escalation procedures
   - b. Telecommunications
   - c. Computer equipment
   - d. Return to primary location

   e. Declaring incident over
      i. Who can declare the incident over?
8. Post test or post event procedures
   a. Capture lessons learned
   b. Improve / update plan
   c. Communicate updated plans
   d. Re-train staff on updated plan
9. Additional considerations
   a. Chain of command (e.g., in the event that management staff is unavailable)
   b. Incidental expenses (e.g., renting conference rooms in a hotel, purchase temporary equipment and supplies, replace damaged equipment)
   c. Post-event reporting
      i. Capturing lessons learned & updating plans
      ii. Expenses – cash, personnel
      iii. Regulatory reporting
10. Appendices
   a. List of Critical and Essential functions
   b. List if IT support systems
   c. Employee contact information
   d. Vendor contact information
   e. External contact information (e.g., emergency support)
   f. Specific procedures
      i. IT and records backup
      ii. IT recovery
      iii. Manual operations
      iv. Evacuation procedures and routes
      v. others.
   g. Test & Drill procedures

5.1.2 Considerations for Returning to Normal Operations

One area of disaster recovery and continuity of operations plans that is often overlooked during plan development is the specific tasks and procedures required to restore normal operations after the disruption is complete. The capability to easily return to normal operations following the use of the backup control center should be a requirement of any new SCADA/EMS procurement; this may require additional applications or the installation of additional features from commercial database applications. Specific procedures will also need to be developed for non-critical and non-essential office functions.

5.1.2.1 Staff

Staff transition can be handled in an orderly and convenient manner. Control room operations can be transitioned by staffing both locations simultaneously, and verifying that all real-time data and operations at the primary location match the same data and operations at the backup location before transferring operations from the backup to the primary. If there are unexplainable differences, the transition back to the primary control center can be deferred until the differences explained or fixed. Control room staff should focus their primary responsibility on continued monitoring and operation, not with relocation activities. Once real-time control is transferred back to the primary control center, staff at the backup location can return to normal operation, and the SCADA/EMS located at the backup control center returned to its normal mode of operation.

Other non-control room staff can also relocate back to the primary control center when convenient to their job schedules. Some staff may assist in re-establishing normal operations at the primary control center as their primary responsibility for a short period of time filling the relocation. These activities are similar to activities performed during a routine office move.

5.1.2.2 SCADA/EMS data

Real-time data will be made available to the recovered site as soon as the telemetry telecommunications links are re-established, and a complete scan is performed. The primary concern when returning to normal operations at the primary control center is maintaining historical data, including alarms, events, manual entries, and application results, that was created or captured at the backup control center during the disruption, and copying it to the primary control center to assure that it is available after the disruptions is over and operations have returned to normal. In configurations other than parallel operations, the backup control center will likely not have a complete copy of the historical data maintained at the primary control center, but will generate future historical data for as long as it has an operational responsibility. This generated data must be copied to the primary control center to maintain a complete historical record of operations.

In extreme cases, where a control center needs to be extensively rebuilt, or the backup has been in operations for a long time, the recovery operation is very similar to the commissioning of a new control system or new control center. This may include creating a physical backup of the SCADA/EMS and its data, and restoring it on the recovering system to start the recovery process.

The actual procedures needed are heavily dependent on the underlying architecture and capabilities of the SCADA/EMS system, as well as the method chosen for the backup control center architecture, as well as the amount of time the backup control center was used for full operations.

If the backup control center is configured as a parallel operations control center, the telecommunications and data synchronization capabilities of the multi-site SCADA/EMS can be used to re-synchronize the data between the two sites. Under normal operations, both control centers must maintain a copy of all data (real-time and historical) used by the SCADA/EMS so that either site can assume complete control with all current data at any time. Following the failure and subsequent recovery of one site, the SCADA/EMS software responsible for maintaining data synchronization should start re-building the data at the recovered site using the re-established high-speed inter-site telecommunication link, while simultaneously maintaining both systems with updated data. This feature is available from commercial database vendors, and is known as “multi-master replication” or “multi-site replication”, and is distinctly different than a “replicated database”. Until the recovered SCADA/EMS is fully restored, operator workstations at the recovered control center could use the telecommunications link and servers at the backup location, allowing the recovered control center to be re-staffed during the data rebuild.

If the backup control center is a hot standby system, it still has high-speed telecommunications that can be used to transfer historical data from the backup SCADA/EMS to the recovered system, but it may take some time before all the historical data is copied from the backup location back to the primary location and made available for use. The longer the backup control center was in operations, the more data will need to be copied back to the primary, and the longer it will take to completely re-build the historical data. The SCADA/EMS would need to have an application that would be able detect and extract the proper historical data and insert it into the running SCADA/EMS at the primary system, meaning that there may be some time when the historical data is unavailable at the primary system. The data replication from the backup control center to the primary control center would need to be performed in parallel with any data updates from the primary control center routed through the backup control center necessary to assure that the backup control center is prepared to take over again if the primary fails (even if the primary is not completely recovered).

If the backup control center is a warm standby or cold standby, the process is similar to the data extraction and insertion process for the hot standby system, except that there is no high-speed telecommunications link between the two control centers. A copy of the historical data would need to be taken (for example, on a DVD), physically transported to the primary control center, and the extraction and insertion application run on the copied data.

PMU data represents a replication and recovery challenge in any of the backup control center scenarios. Unlike telemetry data, PMU data is constantly changing and being streamed to the control center, and it must be captured (or at least processed) constantly in order for it to be of maximum use. The telemetry stream cannot be shut off while the data is copied. It does have the advantage that all the data is time stamped, so the real-time data can be inserted into the PMU database while simultaneously inserting historical data with different timestamps into the same database. The PMU data storage processing must be able to accommodate these different data time streams without causing data storage inefficiencies.

5.1.2.3 Records Data

Electronic copies of records should be stored in an electronic records management system, using an off-premises storage solution. That solution should include contract provisions for redundant storage. Records stored in this manner can be accessed from the primary, backup or any other location, and should remain accessible through the disruption and after the disruption is over in a consistent manner. Hard copy records can be migrated along with staff returning to the primary control center.

5.1.2.4 Other Data

Other electronic and hard copy data, such as finance, payroll, human resources, and corporate records should be manually transported back to the primary control center. Some of these functions may have been relocated to the backup control center, while others may have been relocated to other temporary locations, or performed via teleworking.

5.1.3 Sources for Example Business Continuity Templates:

- Data Center Assistance Group[1].
- AIG Insurance[2]
- United Nations Development Programme[3]:
- Integrated Telemanagement Services, Inc.[4]:
- The U.S. Federal Government's Business Continuity Planning Site[5] (part of the Federal Emergency Response Agency [FEMA] within DHS) includes a program to automatically generate a business continuity plan and a disaster recovery plan geared toward recovering data center resources. The program requests some basic information like company name and contact information for staff, and generates a Microsoft Word document containing a sample plan that can be modified to meet an individual organization's needs.
- U.S. Department of Homeland Security (DHS) PS-Prep™ (private sector preparation) program[6].
- Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions (retired)[7].

6.0 Professional Staff Technical Development

A number of recommendations in this whitepaper may require new or enhanced skill sets for staff. While some tasks, such as design, installation, and initial configuration may be accomplished by third-party contractors and consultants, it is important for the organization to be able to perform ongoing maintenance on new systems. The organization should also consider supporting professional staff obtain and maintain certifications in key areas, specifically cybersecurity, networking, and business continuity. The organization should also support individual or corporate membership in related organizations, and conference attendance as part

[1] See http://www.dcag.com/images/Business_Continuity_Plan_Overview.pdf (accessed 11/30/2020)

[2] See https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/property-insights/business-continuity-planning-guidelines-for-preparation-of-your-plan.pdf (accessed 11/30/2020)

[3] See https://www.google.com/url?client=internal-element-cse&cx=016364595556873131513:lg-p43v3tam&q=http://www.al.undp.org/content/dam/albania/docs/STAR/IT%2520Disaster%2520Recovery%2520Plan%2520Template.pdf&sa=U&ved=2ahUKEwjukYWvxqrtAhXIuZ4KHVOmB0cQFjAAegQIBRAB&usg=AOvVaw2Ky1nt71hhPggoEBy-9BL0 (accessed 11/30/2020)

[4] See https://pronto-core-cdn.prontomarketing.com/2/wp-content/uploads/sites/558/2017/12/its-business-continuity-plan-template-v2.pdf (accessed 11/30/2020)

[5] See https://www.ready.gov/business-continuity-planning-suite (accessed 11/19/2020)

[6] See https://www.fema.gov/pdf/privatesector/FEMA_PS-Prep_One-Pager_Generic.pdf (accessed 11/30/2020)

[7] See https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/WTRMRK-Continuity_Business_Operational_Functions-Retired.pdf (accessed 11/30/2020)

of ongoing education and training activities. Most professional certifications require proof of continuing education to maintain an active certification, which can be at least partially accomplished through such conference attendance and education and training activities.

6.1 Training & Education

Training and education for cybersecurity and business continuity is available from a wide variety of sources. Education is for general cybersecurity topics, while training is generally specific to products or implementations.

There are many sources of educational material for cybersecurity. One of the most popular sources is the SANS Institute[1], which offers online, on-demand, and in-person courses on a wide variety of topics. SANS also offers a complete undergraduate or graduate degree program in cybersecurity[2].

Preparation courses for the CISSP (Certified Information Systems Security Professional), a certification from (ISC)^2 (International Information System Security Certification Consortium) can be sources of general cybersecurity educational material even if a CISSP certification is not desired. Numerous self-paced, on-demand, on-line, and in-person education and training options are available for the CISSP certification.

Preparation courses for the certifications offered by ASIS International[3] are sources of information about physical security, even if obtaining the ASIS certifications is not desired. Course materials include options for webinars, on-line learning, and self-paced instruction are provided on the ASIS website[4].

Self-paced business continuity training is available from the U.S. Federal Government[5] Business Continuity Planning Site. Although some of the materials on the site are intended for wide-scale disaster planning by government organizations, other information is applicable to individual organizations. It can also be used to educate individual organization staff on how government disaster preparedness and response may work.

Nearly all equipment vendors provide training material targeted to their equipment, but also offering basic educational material. For example, training courses from Cisco[6] provide general networking education along with training specific to configuring and maintaining Cisco networking equipment. Training offered by vendors (e.g., Cisco) is often useful preparation for obtaining certifications from that vendor.

6.2 Certifications

The organization should encourage and support technical staff to obtain and maintain certifications in technical areas. These certifications could be general, such as the CISSP, the

[1] See https://www.sans.org/ (accessed 11/19/2020)
[2] See https://www.sans.edu/?msc=main-nav&_ga=2.109871427.796720825.1605818815-1353875011.1604953730 (accessed 11/19/2020)
[3] See https://www.asisonline.org/ (accessed 11/11/2020)
[4] See https://www.asisonline.org/professional-development/education/ (accessed 11/30/2020)
[5] See https://www.ready.gov/business-continuity-planning-suite (accessed 11/19/2020)
[6] See https://www.cisco.com/c/en/us/training-events/training-certifications/training.html (accessed 11/19/2020)

SANS GIAC (Global Information Assurance Certification), the CISM (Certified Information Systems Manager), or they could be specific to a specific product or vendor like the Cisco CCNA (Cisco Certified Network Associate).

6.2.1 Cybersecurity and Physical Security

The primary internationally recognized certificate in cybersecurity is the CISSP[1], issued by the (ISC)[2] organization, which is generally recognized as the cybersecurity equivalent of the U.S. Professional Engineer (PE). In order to receive the certification, an applicant must demonstrate knowledge of eight domains of knowledge, pass an examination (fee required), have five years of industry experience, and be nominated by someone with an existing CISSP certification. The eight knowledge domains are:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

In order to maintain the certification, 120 hours of continuing education are required every three years, along with an annual maintenance fee. (Note – re-taking the examination is also an option, but most holders of the CISSP prefer the continuing education option.)

Another respected certification is the GIAC[2] set of certifications offered by the SANS Institute. Nearly 40 different certifications are available in the following domains[3]:

- Cyber Defense
- Industrial Control Systems (ICS)
- Penetration Testing
- Digital Forensics and Incident Response
- Management and Leadership
- Developer

The GIAC certification process requires passing a timed examination (fee required). Each GIAC certification is valid for four years, after which it must be renewed with a maintenance fee and either continuing professional experience points, publishing a technical paper, or re-taking the exam to extend the GIAC certification for an additional four years. Each separate GIAC certification requires a separate renewal process, although discounts are offered if multiple GIAC certificates are renewed together. The GIAC program also offers a GSE (GIAC Security

[1] See https://www.isc2.org/Certifications/CISSP (accessed 11/11/2020)
[2] See https://www.giac.org/ (accessed 11/11/2020)
[3] See https://www.giac.org/pdfs/GIAC-Program-Overview-2020.pdf (accessed 11/11/2020)

Expert) certification that requires a separate entrance examination, a two-day on-site practical laboratory exercise, and a set of other prerequisites.

Two other certifications offered by the Information Systems Audit and Control Association (ISACA)[1] are the Certified Information Systems Auditor (CISA)[2] and the Certified Information Systems Manager (CISM)[3]. Both of these are more focused on information technology auditing, but also address cybersecurity. ISACA offers other certifications for risk management and governance, and is responsible for maintaining the COBIT (Control Objectives for Information and Related Technologies) framework[4].

The Certified Protection Professional (CPP®) certification is offered by ASIS International. The CPP requires skills in the following areas:

- Security Principles and Practices
- Business Principles and Practices
- Investigations
- Personnel Security
- Physical Security
- Information Security
- Crisis Management

The CPP certification process requires passing an examination (fee required), either seven years of experience, or six years of experience and a bachelor's degree, or five years of experience and a master's degree; have three years in responsible charge of a security function; have been employed full time in a security-related role; and have not been convicted of any criminal offense that would reflect negatively on the security profession, ASIS, or the certification program. CPP certifications are valid for three years, and require 60 continuing professional education credits and a fee to re-certify.

The Physical Security Professional (PSP®) [5] certification is also offered by ASIS International. The PSP requires skills in the following domains:

- Performing threat surveys to evaluate the dangers present at a location or in the organization.
- Design of security procedures and systems.
- Responsibilities of people associated with security and response procedures.
- Setup, operation, and maintenance of security systems.

The PSP certification process requires passing an examination (fee required), either four years of physical experience and a bachelor's degree or six years of experience and high school diploma or associated degree, have been employed full time in a security-related role, and have not been convicted of any criminal offense that would reflect negatively on the security

[1] See https://www.isaca.org/ (accessed 11/11/2020)
[2] See https://www.isaca.org/credentialing/cisa (accessed 11/11/2020)
[3] See https://www.isaca.org/credentialing/cism (accessed 11/11/2020)
[4] See https://www.isaca.org/resources/cobit (accessed 11/11/2020)
[5] See https://www.asisonline.org/certification/physical-security-professional/ (accessed 11/11/2020)

profession, ASIS, or the certification program. PSP certifications are valid for three years, and require 60 continuing professional education credits and a fee to re-certify.

6.2.2 Networking

Many router and firewall equipment manufacturers offer certifications for staff that will be designing and maintaining complex communications networks. For example, Cisco[1] offers a number of certifications at various experience levels[2] including CCNA[3], CCNP (Cisco Certified Network Professional)[4], CCIE (Cisco Certified Internetwork Expert)[5], and CCDE (Cisco Certified Design Expert)[6]. All Cisco certifications require passing an examination (fee required), most require network management experience (advanced certifications require more experience), and some require passing a laboratory practical exercise. Certificates are valid for two to three years, and require recertification including continuing education or re-taking examinations.

Other network equipment vendors may have certifications with their own requirements. Priority should be given to training and certifications from equipment vendors that are used or plan to be used by the organization.

6.2.3 Business Continuity

Business continuity certifications are available from a number of organizations. A 2019 article in Business News Daily[7] lists the following business continuity certifications:

- Certification of the Business Continuity Institute (CBCI)
- Certified Business Continuity Manager (CBCM)
- Certified Business Continuity Professional (CBCP)
- Certified Disaster Recovery Engineer (C/DRE)
- EC-Council Disaster Recovery Professional (EDRP)

The CBCI is offered by the Business Continuity Institute (BCI)[8], a company based in the United Kingdom, and active in Europe, Asia, Africa, and the Middle East. The certification requires passing an exam[9] at the conclusion of a recommended training course (fee required). The training and exam cover the following business continuity topics:

[1] See https://www.cisco.com/ (accessed 11/11/2020)

[2] See https://www.cisco.com/c/en/us/training-events/training-certifications.html (accessed 11/11/2020)

[3] See https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html (accessed 11/11/2020)

[4] See https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-enterprise.html and others (accessed 11/11/2020)

[5] See https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccie-enterprise-infrastructure.html and others (accessed 11/11/2020)

[6] See https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert/ccde.html (accessed 11/11/2020)

[7] https://www.businessnewsdaily.com/10802-business-continuity-disaster-recovery-certifications.html (accessed 11/11/2020)

[8] See https://www.thebci.org/ (accessed 11/20/2020)

[9] See https://www.thebci.org/training-qualifications/cbci-exam.html (accessed 11/20/2020)

- Policy and Programme Management
- Embedding
- Analysis
- Design
- Implementation
- Validation

Additional levels of membership are available: associate (AMBCI, Associate Member of BCI), member (MBCI, full Member of BCI), Associate Fellow (AFBCI) and Fellow (FBCI) levels with fees based on geographic location of the applicant. The CBCI is valid for three years, and requires no exam if the member has advanced their membership level; however, if no membership advancement has taken place, the current CBCI exam must be retaken to maintain the certification.

The CBCM is offered by the Certified Information Security (CIS), located in Florida, U.S. The certification is based on practices in ISO 22301. The CBCM is an expert-level business continuity management certification that requires five years of experience, attending three required training courses (fee required), and passing three exams (fee required). An initial application fee and an annual maintenance fee are required. The CBCM certification is valid for three years, and requires 120 hours of continuing education over the three-year period, and payment of the annual maintenance fee to maintain the certification. CIS also provides training and certifications in risk analysis (based on ISO 31000) and information security (based on ISO 27000), as well as training courses for the CISSP and a variety of fraud control topics.

The CBCP is offered by DRI International and is one of 13 certifications offered. The CBCP includes the following topic areas:

- Program Initiation and Management
- Risk Assessment
- Business Impact Analysis
- Business Continuity Strategies
- Incident Response
- Plan Development and Implementation
- Awareness and Training Programs
- Business Continuity Plan Exercise, Audit and Maintenance
- Crises Communications
- Coordination with External Agencies

The CBCP requires two years of experience in at least five of the topic areas, an application fee, passing an exam (fee required), five topic area essays, and an annual maintenance fee. References are required for the topic areas used for qualification. In-person and self-paced course materials are available (fee required). Recertification is required each year consisting of the annual maintenance fee and continuing education.

The C)DRE is offered by Mile2, and is targeted to the defense industry and to government agencies, and therefore may not be applicable to the organization.

The EDRP is offered by the International Council of Electronic Commerce Consultants (EC-Council), and requires completing a course (fee required) and passing an exam (fee required). No ongoing maintenance fees or education requirements are noted. The EC-Council provides other certifications, the most popular being Certified Ethical Hacker.

6.3 Ongoing Education

Most of the organizations providing training or certifications also offer ongoing education opportunities through webinars, refresher courses, and conferences. Traditionally, many of these opportunities have been “face-to-face”, but have transitioned to virtual events, even for large events in 2020 and 2021. It is not clear whether future conferences and classroom training will return to face-to-face, remain virtual, or become a hybrid of both.

Although ongoing education may be used as continuing education credits to maintain certifications, they can also be a source of additional general knowledge, provide an opportunity to exchange ideas with peers from other organizations, and learn about new and enhanced product offerings.

Other international conferences, like those sponsored by RSA or SANS, offer education and training opportunities, and vendor trade shows like Cisco Live allow participants to discuss their needs with vendors and see product demonstrations in addition to offering education and training. Other organizations, such as the ISA, IEEE, ASIS, ISACA, (ISC)^2, and DistribuTECH also sponsor more general-purpose conferences and trade shows that have cybersecurity, physical security, and business continuity content. If conferences are sponsored by membership organizations, (such as ISA, IEEE, ASIS, ISACA, and (ISC)^2), discounts on conference registration are offered to members.

Pacific Northwest
National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov