ITEGRITI

CRITICAL INFRASTRUCTURE PROTECTION
cybersecurity + compliance + managed services

ITEGRITI Corporation
2101 CityWest Boulevard
Suite 100
Houston, TX 77042

April 2023

PROTECTING THE BES FROM MODERN THREATS:

Is NERC CIP Compliance Enough?

By Dr. Thomas "Tom" Duffey,
ITEGRITI Director of Cybersecurity and Compliance

 |

Table of Contents

Critical Infrastructure

Based on the United States (U.S.) Executive Order 13010, critical infrastructure consists of specific national systems whose destruction or incapacitation could potentially harm economic security (Duffey, 2018). The United States (U.S.) Cybersecurity and Infrastructure Agency (CISA) has defined 16 critical infrastructure sectors with essential physical and virtual assets, systems, and networks.

Operational technology (OT) includes industrial control systems (ICSs) such as supervisory control and data acquisition (SCADA) devices, energy management systems (EMSs), and distributed control systems (DCSs), which monitor, control, and access operational and industrial equipment. These devices, including control systems for critical infrastructure, differ from traditional IT equipment and use specialized hardware and software.

ICSs used for various industries vary globally, but the core mission of using these devices is to control and automate operational tasks. Historically, they were standalone "air-gapped" systems using serial protocols and running customized operating systems, but modern ICSs include Internet-facing connections, creating significant challenges and providing potential rogue actors and nation-states with excessive access and new avenues for cyber-attacks in the energy industry.

The Bulk Electric System

According to Presidential Policy Directive (PPD) 21, government and private sector organizations own and operate about 90% of this critical infrastructure, including the electric energy sector (Duffey, 2018). Bulk Electric System (BES) infrastructure consists of three separate U.S. electric interconnections encompassing the East, the West, and Texas. These interconnections, composed of multiple energy-related cyber assets responsible for generating, transmitting, and distributing U.S. electric sector power, represent a vital cyber-attack target for rogue entities or enemy nation-states.

Electric entity control centers manage multiple essential processes and demand adjustments across the electric grid, communicate with substations, control circuit breakers, and balance power while monitoring and responding to potential events, faults, and incidents. Ensuring BES reliability is critical to national security and safety because attacks could potentially cause damage and escalate into widespread physical destruction, shutting down vital services and disrupting routinely sustainable fundamental functions, including transportation, water and food supplies, and telecommunications (Duffey, 2018).

Continuously Evolving Threats

Enhanced network connectivity has increased risk and susceptibility. In recent years, multiple cyberattacks on operational technology (OT), including SCADA and other industrial control systems (ICS), which monitor, control, and access operational and industrial equipment, have made national and international headlines.

Based on analysis of successful cyberattacks impacting the U.S. and other countries, the White House, Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and other agencies have confirmed the potential for more severe BES consequences, possibly resulting in significant power outages impacting large populations for extended periods. **Appendix B** contains a non-exhaustive and growing list of sample incidents and warnings from the previous decade and a half, illustrating the global danger and impact of physical and cyberattacks on critical energy infrastructure. This subset of events demonstrates that coordinated cyberattacks are increasing, leveraging combined threat vectors and simultaneously targeting multiple IT and OT vulnerabilities.

A 2022 joint cybersecurity advisory from the U.S. (DOE), Cybersecurity and Infrastructure Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) revealed that advanced persistent threats (APT) threat actors now have custom-made automated malware named Pipedream/INCONTROLLER, which targets ICSs and SCADA systems. This advisory

2018	Denmark	NotPetya malware leveraged a Microsoft Windows master boot record exploit to shut down operations for six days.
	Saudi Arabia	During an unsuccessful attack designed to put lives at risk, Triton malware (which could have potentially caused explosions or released toxic gas) attempted to take control of safety instrumented systems at a petrochemical plant.
	USA	The FBI and DHS issued a joint technical alert, including indicators of compromise (IOCs) and techniques, for recent nation-state efforts targeting the U.S. government and critical infrastructure for energy, nuclear, water, aviation, manufacturing, and more.
	Ukraine, Poland	GreyEnergy malware with advanced stealth capabilities, including AES 256-bit encryption and "fileless" modules, ran in the memory and targeted SCADA workstations.

strongly encouraged critical infrastructure protection bolstering through multifactor authentication, password strengthening, and continuous OT monitoring solutions for specific programmable logic controllers (PLCs) and servers (CISA, 2022).

Regulatory Compliance Mandates

Compliance encompasses local, state, federal, and international laws, regulations, and standards. These requirements, which target various industry and government verticals, sectors, and even countries, contain multiple mandatory management, operational, and technical "controls" (i.e., countermeasures) to help mitigate organizational risk. Legal and regulatory compliance documentation development usually involves multiple "drafting team" participants contributing collectively.

Compliance mandates may take weeks, months, or years to receive final approval, accompanied by a "waiting period" before actual enforcement. Due to the dynamic and constantly evolving nature of cyber threats, by the time all the proverbial "red tape", and signatures are in place, the content of a law or regulation may be on its way to obsoletion. For this reason, compliance is often considered the "floor" of information security. After implementation, regulatory bodies may conduct periodic audits, inspections, "spot checks", and/or "self-reports". The most important thing to understand about compliance is that it is usually mandatory, and meaningful penalties and/or monetary fines often accompany non-compliance.

Security Frameworks

Unlike mandated compliance and privacy laws and regulations, security frameworks comprise industry and government "best practices." Security frameworks consist of "optional" or "recommended" security controls and sub-controls, grouped into management, operational, and technical "families" of security controls and sub-controls. In contrast to compliance and privacy controls, which are usually more general, security controls are more granular and prescriptive. Some security frameworks facilitate "tailoring" and/or "overlays" to increase security posture robustness. Participation is voluntary, with no penalties or monetary fines for non-use.

Implementation of a security framework starts with categorizing organization information systems and classifying the data they store, transmit, and process. Applicable security control families, controls, and sub-controls are chosen and implemented based on their design and ability to mitigate organizational risk. Due to the dynamic and ever-evolving threat landscape, security controls may "atrophy" or lose their value over time. Organizations must periodically test these security controls and sub-controls to verify their ongoing efficacy.

Bulk Electric System Safety and Reliability

Any threat to electric entities is a danger to everyone involved with them, and security is everyone's responsibility organization-wide, starting top-down with management. Different utilities are at various stages along a regulatory compliance continuum, ranging from non-compliance or maintaining compliance to a more mature sustainable position moving toward optimization and advanced security for higher-risk BES Cyber Assets (BCAs) and BES Cyber Systems (BCSs). Two sets of mandated cybersecurity compliance criteria that help electric entities achieve their goal of keeping the proverbial lights on before, during, and after cyber incidents are the NERC CIP standards and TSA security directives.

NERC Critical Infrastructure Protection Standards

In response to Federal Energy Regulatory Commission (FERC) Order 706, the North American Electric Reliability Corporation (NERC) created a series of nine mandatory critical infrastructure protection (CIP) regulatory compliance standards to improve the U.S. Bulk Electric System (BES) reliability and security (NERC, 2023). These standards, which require both internal assessments and external audits, are continually revised and updated to accommodate new cyber risks. Since then, additional FERC-ordered mandates have been added, accompanied by new and revised CIP standards.

NERC developed CIP-013 in response to FERC Order 829, addressing increased cyberattacks targeting the supply chain, including concerns about the "insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, and inadequate safety measures in manufacturing and development practices" (FERC, 2018). Some counterfeit devices may include forged tagging for safety, engineering, and manufacturing regulations, creating significant concerns (Control, 2019).

Due to armed attacks on a Metcalf, CA substation, NERC developed CIP-014 to enhance physical security protection for transmission stations, substations, and associated control centers. Recognizing the importance of situational awareness that control center communications play in BES reliability led to FERC Order 822 (FERC, 2016). Subsequently, NERC developed CIP-012, requiring electric entities to develop plans and controls to mitigate the risk of potential unauthorized disclosure and modification of real-time data transmitted between control centers.

The current NERC CIP suite (see **Appendix C**) includes 13 regulatory documents with multiple mandatory requirements, a matrix of assigned Violation Risk Factors (VRFs), Violation Severity Levels (VSLs), and steep non-compliance fines of up to $1 million per day per occurrence. These compliance standards address physical security and cybersecurity for the BES, including generation, transmission, energy management systems, control centers, supply chain, etc., and FERC compliance requirements (NERC, 2023).

Standard	Effective Date	Cybersecurity Compliance Area
CIP-002-5.1a	12/27/2016	BES Cyber System Categorization
CIP-003-8	04/01/2020	Security Management Controls
CIP-004-6	07/01/2016	Personnel & Training
CIP-005-7	10/01/2022	Electronic Security Perimeter(s)

FERC continues to create additional cybersecurity requirements for NERC to implement based on the current threat landscape. Most recently, in January 2023, FERC released a final rule requesting that NERC submit new or modified standards addressing Internal Network Security Monitoring (INSM) for High and Medium BES cyber systems (BCSs) with external routable connectivity (ERC) while concurrently conducting additional INSM research for other types of BCSs (FERC, 2023).

TSA Pipeline Security Directives

BES supply chain risks subject to cyber-attacks include natural gas pipelines supplying electric entities. In response to the 2021 Darkside ransomware attack, the Transportation Security Authority (TSA) updated previous guidelines and published Security Directive Pipeline-2021-01 (SD01) containing mandatory pipeline security requirements. A few months later, the TSA released Security Directive Pipeline-2021-02 (SD02B), categorized as Security Sensitive Information (SSI) with access restricted to pipeline owners and operators, containing more prescriptive hardening requirements for pipelines (TSA, 2022).

Unfortunately, some of the more stringent compliance-based requirements in SD02B did not work well for OT systems. The TSA leveraged lessons learned by collaborating with pipeline owners and operators, industry groups, and other government partners to develop Security Directive Pipeline 2021-02C (SD02C), which takes a more flexible performance-based approach. SD02C, the current iteration aligns well with other security frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443. This regulation impacts multiple verticals, including electric entities and, ultimately, the BES.

NERC continues to publish and revise new standards, and the TSA pipeline security directive has evolved through three iterations since the initial release. These two mandated cybersecurity compliance criteria help keep the proverbial lights on. However, they are different, and each brings value with enhancements not included in the other (see **Appendix D**). As shown in **Figure 1**, approximately 24% of the TSA SD02C requirements not included in NERC CIP-005-7 help boost electronic security. Conversely, 14% of the CIP-006-6 control enhancements not addressed by SD02C fall under the physical security category (see **Figure 2**). Almost one-third of TSA control enhancements focus on system security, which falls under CIP-007-6, the most commonly violated standard in the NERC suite.

- Zoned architecture based on criticality, consequence, and operational necessity
- Initial 24-hour network traffic capture (PCAPs), as identified and directed by TSA, providing a "snapshot" of activity on and between IT and OT systems
- Ongoing “snapshots" of activity on and between IT and OT systems (e.g., log files)

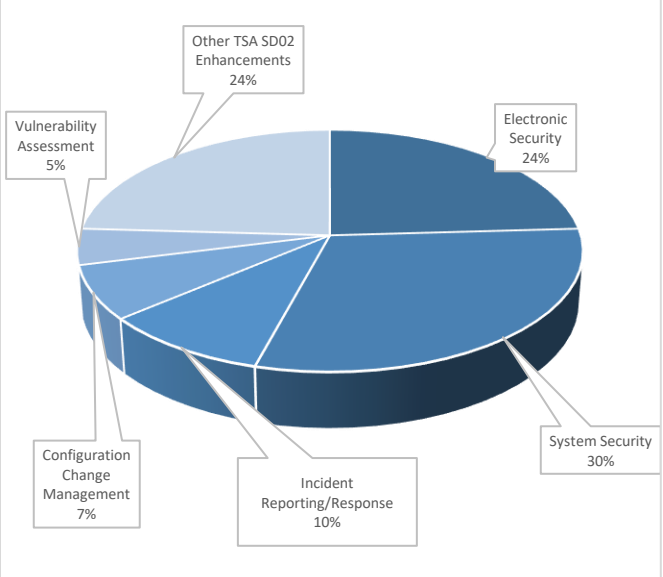

Figure 1: *TSA SD02 Enhancements Over CIP*

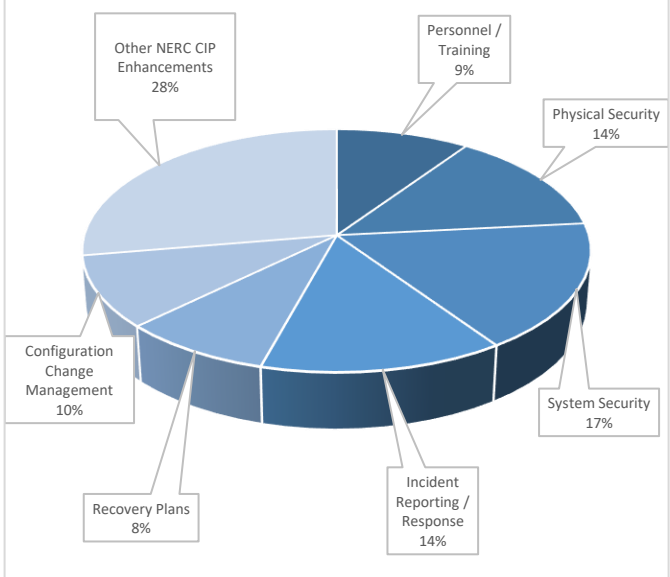

Figure 2: *NERC CIP Enhancements Over SD02*

Electric entities invest heavily in time, and energy spent interpreting compliance mandates and defining required policies, procedures, processes, roles and responsibilities, and technical controls to help assure compliance. However, despite the name "cybersecurity" being used throughout NERC CIP and TSA SD02, utilities must understand that compliance is not security, and security is not compliance. However, compliance may leverage security controls and vice versa.

Compliance and Security Challenges

People, processes, and technology are essential to successful compliance and security. Formal buy-in and approval start with upper management support, proper governance, risk, compliance program, and acceptance at other organizational levels. Attaining and maintaining mandatory compliance can be expensive and time-intensive, but so can the consequences of failing to do the right thing. More importantly, approaching compliance from a fragmented perspective may result in significant gaps, increased risk, and potential financial and credibility consequences. Some common challenges electric entities may struggle with at the more general program level include but are not limited to:

- NERC CIP and TSA SD02 compliance program management, planning, and scheduling
- Ensuring organization-wide compliance ownership is known, implemented, and documented
- Regulatory compliance verbiage and interpretation challenges
- Robust management, collaboration, and compliance reporting
- Thorough identification of management, operational, and technical gaps
- Defining and executing timely prioritized remediation plans
- Alignment of audit artifacts with NERC Evidence Request Tool (ERT) requirements
- Proper preparation and planning for NERC CIP audits
- Evidence collection, quality, and timeliness, along with compliance status tracking
- Human resources, attrition, and budgeting challenges
- Advancing beyond NERC CIP and TSA SD02 compliance to achieve advanced security

Electric entities must use a proactive and strategic approach to compliance and security, leveraging sustainable management, operational, and technical controls. Unfortunately, some utilities with the "checklist" mentality may establish reactive and non-integrated regulatory compliance programs using non-sustainable processes focused on incremental implementation and reporting solutions. This mindset creates barriers to building a comprehensive, supportable, repeatable, efficient, and automated evidence management program required to achieve compliance, mitigate risk, and protect critical infrastructure. **Appendix E** shows some of the more significant compliance challenges utilities commonly face.

Electronic Security Perimeter(s)	• Creating proper segmentation using a zoned "zero trust" architecture, effectively separating IT systems from OT systems
Physical Security of BES Cyber Systems	• Robust layered physical security for IT and OT assets and systems
System Security Management	• OT asset and system compliance with the more IT-rooted technical NERC CIP standards and SD02-mandated requirements

Meeting and overcoming these regulatory compliance and security challenges requires process standardization and repeatability gained through integration and automation. Standardizing and automating processes with higher levels of effort, like evidence collection, validation, and reporting, along with exception management, improves efficiency and moves utilities along the maturity curve. By leveraging automated workflows and proactive alerting, electric entities can help mitigate the risk of non-compliant, outstanding, and overdue NERC CIP and TSA SD02 requirements. Leverage an ongoing governance program that manages regulatory compliance and determines the impact of revised requirements, new NERC CIP standards, and mandatory enforcement dates.

Optimization

Different utilities are at various stages along a regulatory compliance continuum, ranging from non-compliance or maintaining compliance to a more mature sustainable position moving toward optimization and advanced security for higher-risk cyber assets and systems. Optimization requires understanding regulatory compliance needs and goals, performing a current state assessment, analyzing existing processes and controls, and evaluating potential efficiency and automation opportunities. Target high-value areas, using assessment methodologies to help identify tasks and operations candidates with the highest levels of manual effort.

Electric entities must understand and comply with current, revised, and new regulatory standards and directives to improve compliance maturity and sustainability. They must also address significant gaps and build the foundational components of a robust compliance program, including more efficient automated and repeatable processes for evidence collection and compliance demonstration. Reducing inefficient and costly manual and time-consuming processes will help lower required effort and time, freeing staff up for other tasks.

Moving the proverbial needle from “old-school” checklists to more efficient compliance and security further reduces organizational risk to the BES. Optimization helps increase evidence consistency, quality, completeness, and timeliness, mitigating the risk of potentially significant violations and penalties for non-compliance. Potential benefits of this approach include greater operational control, better management, lower maintenance costs, improved situational awareness, reduced risk, better contingency planning, and more robust safety, security, and reliability.

The ability to dynamically adjust to current regulatory compliance needs helps improve efficiency while reducing operational expenditures (OPEX), capital expenditures (CAPEX), and unnecessary overhead. NERC CIP and TSA SD02 controls require tests of design before implementation, along with ongoing viability and effectiveness oversight. Many compliance activities are periodic (e.g., patching, training, access and authorization reviews, cybersecurity vulnerability assessments, incident response testing, and recovery testing). Qualified third-party assistance helps utilities meet compliance requirements when they are most needed. Leveraging flexible critical infrastructure protection services from these firms allows staff to focus on their core roles and responsibilities.

Advanced Security: Compliance Alone is Not Enough

Attackers routinely breach fully compliant infrastructures and systems meeting regulatory requirements. Genuinely protecting the BES requires moving beyond compliance, which many auditors consider the baseline for cyber health (Duffey, 2018). Advanced security involves leveraging a concept of operations (CONOPS) spanning the entire business, encompassing the people, processes, procedures, stakeholders (and their responsibilities), tools, and technologies underpinning electric entity compliance and security programs.

Compliance and security should not operate in a vacuum. Breaking down traditional “silos” and opening lines of communication fosters collaboration and facilitates streamlining regulatory compliance and security efforts. Co-creation, design thinking, and cross-training allow utilities to leverage resources across the organization. Identify control owners (accountable business stakeholders) for specific NERC CIP standards and/or TSA SD02 compliance requirements. Advanced security, especially for high-risk assets, requires the collaboration of physical security and cybersecurity stakeholders, making security intrinsic to every area of utility operations.

To illustrate the importance of advanced security, consider a manual process for tracking access authorization meeting CIP-004-6, CIP-005-7, and CIP-007-6 requirements. This process relies on human intervention and may lead to stagnation, atrophy, and errors. In contrast, automated identity and access management systems, privileged access management tools, and password vaulting applications provide better and more mature protection.

Compliance and security professionals must keep pace with the dynamically changing threat landscape by

deploying more progressive strategies and increasing robustness and cognitive security tools. For example, security events logging using a traditional Security Information and Event Management (SIEM) solution might comply with current CIP standards (CIP-007-6, CIP-008-6, CIP-011-2). However, advanced protection requires a more advanced monitoring system integrated with a broader cybersecurity operations center using a Security Orchestration, Automation, and Response (SOAR) event correlation system. SOAR (a requirement for TSA SD02C compliance) uses artificial intelligence (AI) and machine learning (ML) to help predict potential broader incidents.

Technology is continually advancing, and globally cybercriminals are stepping up their game. The Ransomware-as-a-Service (RaaS) business model is highly successful. RaaS is relatively inexpensive, uses a subscriber-based licensing model (similar to popular cloud service offerings), and requires minimal deployment skill. Last year, ransomware attacks on utilities and manufacturing cost businesses over five billion dollars, and the numbers are rising (Bischoff, 2023). Insider threat attacks have also increased in recent years.

Business email compromise (BEC) seriously threatens organizations, including utilities. According to the FBI Internet Crime Complaint Center (IC3), BEC-related losses amounted to 49 times those from ransomware. Between 2020 and 2021, a seven percent increase in BEC compromises resulted in almost $7 billion in potential losses, approximately one-third of total cybercrime cost (FBI, 2021). BEC is a social engineering scheme that targets high-profile individuals from multiple industry verticals, attempting to defraud the organization to obtain financial or sensitive information (Proofpoint, 2023).

An “insider” is anyone with past or present access to or knowledge of electric entity facilities, networks, systems, assets, or personnel (CISA, 2023). Negligent insiders may lack security awareness or be unintentionally prone to human error, but malicious insiders usually seek some form of personal or monetary gain. Hollywood movies have portrayed insiders as disgruntled employees seeking payback or revenge. In reality, the threat may not originate from within the organization. Third-party contractors and vendors with uncontrolled interactive or remote access to cyber assets may covertly access and compromise critical infrastructure while going unnoticed (Uniserve, 2023).

As cyberattacks like these continue evolving, accompanied by increased demands on compliance and security teams, electric entities need a trusted partner to help keep their IT and OT environments compliant, safe, and reliable. ITEGRITI collectively brings a team of professionals with decades of experience consulting across multiple commercial and government industry verticals.

Do you know your Security Maturity Level? Find out here:

https://itegriti.com/cybersecurity-risk-baseline

ITEGRITI specializes in cybersecurity, compliance, and managed services. Our clients bring us some of their most crucial issues to solve, and we have extensive experience helping protect some of the nation's most critical infrastructure assets. Our team provides actionable recommendations to help improve their cybersecurity and compliance programs and manage their risks more effectively. See **Appendix A** to learn more about how we may help with your cybersecurity and compliance needs.

References

1 Bischoff, P. (2023, March 7). Ransomware attacks on US manufacturing and utility businesses cost $5.53bn in 2022. *Comparitech*. Retrieved from https://www.comparitech.com/blog/vpn-privacy/ransomware-attacks-manufacturing-utilities/.

2 Control (2019, May 29). *Yokogawa announcement warns of counterfeit transmitters*. Retrieved from https://www.controlglobal.com/measure/pressure/news/11301415/yokogawa-announcement-warns-of-counterfeit-transmitters.

3 Cybersecurity and Infrastructure Security Agency. (2022, September 22). *Control system defense: Know the opponent.* [Cybersecurity Advisory]. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-265a.

4 Cybersecurity and Infrastructure Security Agency. (2023). Defining insider threats. Retrieved from https://www.cisa.gov/defining-insider-threats.

5 Duffey, H. T. (2018). *A qualitative phenomenological study explores the impact of NERC CIP regulatory compliance on risk and security for Bulk Electric System grid cyber-attacks*. (Doctoral dissertation). Retrieved from https://pqdtopen.proquest.com/doc/2176028631.html?FMT=ABS.

6 Federal Bureau of Investigation. (2021). *Internet crime report 2021*. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

7 Federal Energy Regulatory Commission. (2008, January 18). Order No. 706: *Mandatory Reliability Standards for Critical Infrastructure Protection*. Retrieved from https://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf.

8 Federal Energy Regulatory Commission. (2016, January 21). Order No. 822: *Revised Critical Infrastructure Protection Reliability Standards*. Retrieved from https://www.ferc.gov/whats-new/comm-meet/2016/012116/E-2.pdf.

9 Federal Energy Regulatory Commission. (2018, October 18). Order No. 829: *Revised Critical Infrastructure Protection Reliability Standards*. Retrieved from https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf.

10 Federal Energy Regulatory Commission. (2023, February 9). Final Action: *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*. Retrieved from https://www.federalregister.gov/documents/2023/02/09/2023-01453/internal-network-security-monitoring-for-high-and-medium-impact-bulk-electric-system-cyber-systems.

11 North American Electric Reliability Corporation. (2023). US Reliability Standards. Retrieved from https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx.

12 Pekoske, D.P. (2022, July 1). *Revision to the Security Directive Pipeline-2021-02 series: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing.* [Memorandum]. Transportation Security Authority. Retrieved from https://www.tsa.gov/sites/default/files/tsa_sd_pipeline-2021-02-july-21_2022.pdf.

13 Proofpoint (2023). *Business Email Compromise (BEC)*. Retrieved from https://www.proofpoint.com/us/threat-reference/business-email-compromise#:~:text=Business%20email%20compromise%20(BEC)%20is,every%20industry%20around%20the%20world.

14 Uniserve (2023). *How to protect your business from insider threats.* Retrieved from https://uniserveit.com/blog/how-to-protect-your-business-from-insider-threats.

Appendix A: ITEGRITI Security and Compliance Capabilities

We understand Critical Infrastructure Protection and are here to help.

At ITEGRITI, we partner with our energy clients, build long-term relationships, and assist them with cybersecurity, compliance, and managed service needs. Reaching optimal levels of advanced security beyond minimal NERC CIP and/or TSA SD02 compliance might seem daunting to utility leaders with more constrained resources and budgets. But our team is here to help.

Our team has developed a broad perspective working with various OT/ICS entities, including Oil and Gas (O&G) clients, Independent Power Producers (IPPs), integrated utilities, municipalities, cooperatives, and transmission companies across all NERC regions. Additionally, ITEGRITI attends vital conferences and workshops. We are active within multiple industry-sharing groups, maintaining functional relationships with the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Our staff also endeavors to stay current with critical infrastructure security trends. Because of this, ITEGRITI monitors the ever-evolving trends to improve cybersecurity, combined with our experience.

As a leader in critical infrastructure protection, ITEGRITI delivers services across the NERC CIP and TSA SD02C landscape, assisting with documentation review/creation, compliance gap analysis, vulnerability assessments (VAs), efficiency/automation reviews, audit readiness, and more.

Proactive Knowledge

Our NERC CIP and TSA subject matter experts (SMEs) provide a wealth of knowledge and experience with multiple compliance regulations and security frameworks, offering sound advice and helping clients interpret and implement challenging requirements and security controls. ITEGRITI leaders and project managers leverage their decades of experience to protect critical client infrastructure.

Critical Infrastructure Protection Assessment

Our team includes multiple qualified and certified SMEs (and subject matter advisors) with expertise in performing risk assessments within IT/OT environments. We help identify gaps and opportunities for improvement and provide a roadmap with milestones to help achieve NERC CIP and TSA SD02 compliance and security maturity using proven ITEGRITI tools, techniques, and practices.

Security Control Implementation

ITEGRITI brings to the table the experience and know-how to assist with required compliance and security documentation, enabling staff to focus on daily operations. These tasks include creating and revising CIP- and TSA-compliant policies, procedures, process maps, flow diagrams, and other strategic and tactical documentation. Additionally, our staff of experienced subject matter experts assists with implementing required management, operational, and technical controls.

Audit Readiness

Our professionals have experience working with both regulations and auditors. The 2022 ITEGRITI CIP field audit guide explains the audit process from inception to completion. We help clients prepare for upcoming audits, starting with a risk assessment to identify potential documentation and technical gaps and assisting with risk remediation tasks. We also assist organizations with completing pre-audit Reliability Standard Audit Worksheets (RSAWs) and NERC Evidence Request Tool (ERT) requirements, preparing evidence artifacts, and creating a Plan of Action and Milestones (POA&M) with individual mitigation action plans (MAPs).

Continuous Monitoring

We collaborate with your team to align cybersecurity and regulatory compliance requirements with the risks specific to your organization. To provide the most significant cybersecurity benefit, we establish and evaluate specific risk metrics, measure the operational effectiveness of existing controls, develop an improvement and remediation plan, and execute those activities.

Compliant and Secure Environment Maintenance

ITEGRITI helps organizations determine the implications of new and revised regulatory requirements and the latest trends in advanced security. Our team can review and assist with required documentation and technical control revisions.

Your Trusted Partner

We enjoy long-term collaborative partnerships and assist our clients with CIP/TSA compliance and advanced security. Our team has provided OT/ICS compliance services, including NERC CIP expertise, for multiple industry sectors since 2006. We bring a tailored approach to each client. ITEGRITI has assisted numerous energy clients with cybersecurity and compliance needs.

Appendix B: Sample Critical Infrastructure Attacks

Year	Geographical Impact	Cyberattack Summary
2008	USA	An energy entity hired a "penetration-testing consultant" whose actions impacted operations and exposed the company's Internet connectivity as a critical vulnerability.
	Poland	A teenage student used a homemade device to control ICSs, derail public trams, and cause crashes.
	Multiple Global Countries	Extortionists attacked overseas electrical utilities in various cities, demanding payments before power disruption.
2009	USA	Nation-state threat actors used a phishing attack to launch Operation Aurora against Google and other organizations from various industry verticals.
2010	Iran	The infamous Stuxnet computer virus was covertly inserted into SCADA equipment controlling ICSs for more than 1K nuclear uranium enrichment program centrifuges, causing malfunction, destruction, and significant political consequences.
2011	USA, Greece, Kazakhstan, Taiwan	Night Dragon trojan attacks targeted and assumed remote control of ICSs at significant global oil, petrochemical, and energy entities.
	Australia	A disgruntled former employee initiated a wastewater attack on ICSs, attempting to convince the water treatment company to employ him to "solve" the problems he was creating.
2012	Saudi Arabia	The Shamoon virus infected more than 30K ICSs at an oil company, erasing all the data on computer hard drives and resulting in severe and irreparable damage.
	Middle East	With cyber espionage capabilities, the Flame virus exfiltrated large amounts of data (believed to have been active for approximately two years before detection).
2013	USA	Cybercriminals exploited a modem connection vulnerability to obtain water-level and temperature information for the New York Rye Brook dam, failing to operate the floodgate remotely but demonstrating infrastructure vulnerability.
	USA	Snipers fired on a California electrical substation, knocking out 17 giant transformers and highlighting the risk and severity of physical attacks on an electric entity. (*Note: More than 50 percent of attacks reported to the Department of Homeland Security in 2013 were directed at energy entities, making it the most-targeted sector for cyberattacks*).
2014	USA, Canada, Europe	An Energetic Bear (Dragonfly) cyber-espionage campaign infected multiple ICSs at energy, aviation, and defense companies, gaining complete control using various malware and collecting data using trojan backdoors.
	Belgium, Germany, Switzerland	88 Havex remote access trojan (RAT) variants compromised ICS software from three major vendors.
2015	Global	Multiple cyberattacks on Supervisory Control and Data Acquisition (SCADA) systems included control center lockouts and ransomware attacks requiring payment to regain control of utility ICSs.
	Ukraine	Sophisticated BlackEnergy ICS malware attack malware facilitated remote control, shutdown, password changes, and account lockout, affecting almost a quarter of a million customers.
	Ukraine	A subsequent BlackEnergy attack using the KillDisk disk-wiping component impacted Ukrainian mining and railway systems.
2016	USA	A joint analysis report by the FBI and DHS detailed tools and infrastructure used by Russian intelligence to compromise the United States government, political, and private sector networks.
	Ukraine	An advanced Crash Override attack launched against two utilities used software backdoors, customized Industroyer malware, and help-desk denial-of-service attacks, to disconnect multiple substations, impacting almost a quarter of the Ukrainian power grid.
	Ukraine	A sophisticated BlackEnergy attack impacted almost a quarter million customers through reconnaissance, customized ICS-impacting malware, and a help desk denial-of-service attack.

2017	USA	VPNFilter advanced modular malware used to initially target Ukraine infected more than 500K routers and network-attached storage devices, scanned multiple ports, monitored SCADA protocols, exfiltrated website credentials, and rendered multiple devices useless.
	USA	A spear-phishing campaign used advanced malware-compromised networks to search for SCADA information, including reference documents, wiring diagrams, and panel layouts.
	Denmark	NotPetya malware leveraged a Microsoft Windows master boot record exploit to shut down operations for six days.
	Saudi Arabia	During an unsuccessful attack designed to put lives at risk, Triton malware (which could have potentially caused explosions or released toxic gas) attempted to take control of safety instrumented systems at a petrochemical plant.
2018	USA	The FBI and DHS issued a joint technical alert, including indicators of compromise (IOCs) and techniques, for recent nation-state efforts targeting the U.S. government and critical infrastructure for energy, nuclear, water, aviation, manufacturing, and more.
	Ukraine, Poland	GreyEnergy malware with advanced stealth capabilities, including AES 256-bit encryption and "fileless" modules, ran in the memory and targeted SCADA workstations.
2019	USA	Nation-state threat actors launched a spear-phishing malware attack against three significant electric entities.
	USA	An external threat actor exploited a known firmware vulnerability on Internet-facing firewalls, causing unexpected reboots and controlling communications, resulting in denial-of-service conditions at a low-impact control center and multiple remote low-impact generation sites.
	India	Personnel detected malware in nuclear power plant networks.
2020	USA	SolarWinds Orion software distributed malware that compromised multiple industrial control system supply chains, including those controlling turbines, over an extended period.
	Europe	EKANS ransomware, which stops Windows ICS processes before encryption, targeted multiple industry verticals, including energy, manufacturing, and automotive operations.
	Israel	Multiple unsuccessful cyberattacks attempted to modify water chlorine levels, leading the Israel National Cyber-Directorate (ICND) and Water Authority to encourage password changes for water treatment facilities (especially chlorine control devices).
2021	USA	Cybercriminals leveraged a workstation human-machine interface (HMI) to remotely change sodium hydroxide (NaOH) levels for a Florida city municipal system, attempting to poison the water supply.
	USA	A DarkSide ransomware attack on a significant pipeline spanning from Texas to New Jersey leveraged a dormant virtual private network (VPN) account and halted production, leading to an acute fuel shortage and exponential price increase (*Note: This attack, impacting U.S. critical infrastructure spanning several states, was the largest publicly disclosed OT/ICS incident*).
2022	USA	According to a FLASH alert from U.S. security agencies and the Department of Energy (DOE), AlphaV (a.k.a. BlackCat) ransomware leveraged Microsoft Group Policy Objects (GPOs) to successfully hack over 60 organizations, including one of Houston's largest private oil and gas companies.
	USA	Combined physical substation attacks in Washington and North Carolina led to approximately 60K power outages.
	Iran	Predatory Sparrow (Gonjeshke Darande) hacktivists conducted multiple attacks halting production at steel companies and gas stations.

Table 1: *Representative sample of critical infrastructure cyber attacks*

Appendix C: Currently Enforceable NERC CIP Standards

Standard	Effective Date	Cybersecurity Compliance Area
CIP-002-5.1a	12/27/2016	BES Cyber System Categorization
CIP-003-8	04/01/2020	Security Management Controls
CIP-004-6	07/01/2016	Personnel & Training
CIP-005-7	10/01/2022	Electronic Security Perimeter(s)
CIP-006-6	07/01/2016	Physical Security of BES Cyber Systems
CIP-007-6	07/01/2016	System Security Management
CIP-008-6	01/01/2021	Incident Reporting and Response Planning
CIP-009-6	07/01/2016	Recovery Plans for BES Cyber Systems
CIP-010-4	10/01/2022	Configuration Change Management and Vulnerability Assessments
CIP-011-2	07/01/2016	Information Protection
CIP-012-1	07/01/2022	Communications between Control Centers
CIP-013-2	10/01/2022	Supply Chain Risk Management
CIP-014-3	06/16/2022	Transmission Stations, Substations, and Control Center Physical Security

Table 2: *Currently Enforceable NERC CIP Regulatory Standards*

Appendix D: NERC CIP Compared to TSA SD02C

Cybersecurity Compliance Area	TSA SD02 Control Enhancements to Mandated NERC CIP Requirements	NERC CIP Control Enhancements to Mandated TSA SD02 Requirements
Cyber System Categorization and Inventory	• Classification of all IT and OT assets/systems • Inventory of all hardware, software, and SCADA systems • Government documentation approvals	• "Brightline" asset classification criteria • Asset categorization process reviews
Security Management Controls (Documentation, Assignment, Delegation)	• MAIN REQUIREMENT #1: ○ TSA Cyber Implementation Plan (TCIP) • Index of records in the same sequence as directive requirements • Compliance record availability • TCIP updates within one year of the previous submission • Formal TSA amendment requests for Owner/Operator changes, documentation changes, and new/additional capabilities	• CIP Senior Manager approval of cybersecurity documentation • Policy and plan implementation, reviews, and updates • CIP Senior Manager assignments and changes • CIP Senior Manager Delegations of Authority
Personnel and Training [Awareness, Training, Personnel Risk Assessments, Access Management]	• NIST SP 800-53 compliant access control • Access based on the principles of "least privilege" and "separation of duties" • NIST SP 800-63 compliant privileged accounts for IT and OT systems (approved verbally and ongoing need documented) • Access reviews every 90 days • Shared account password changes within seven days of employment changes	• Security awareness • Security training (initial and refresher) • Required training before granting electronic and physical access • Personnel risk assessments • Periodic access authorization record verification • Periodic BCSI storage location access verification • Electronic, physical, and BCSI storage access removal for terminations • Electronic and physical access revocation for transfers/reassignments • Non-shared user account revocation for terminations
Electronic Security Perimeter(s) [Architecture, Electronic Access Point(s), Electronic Perimeter Security, Remote Access]	• IT and OT system interdependency identification • Identification of external connections to OT systems • Lists of publicly routable IP addresses and VLANs • Allowlisting for OT systems with Internet access • Network segmentation policies/procedures to isolate OT systems from IT systems in the event of a compromise • Zoned architecture based on criticality, consequence, and operational necessity • Initial 24-hour network traffic capture (PCAPs), as identified and directed by TSA, providing a "snapshot" of activity on and between IT and OT systems • Ongoing "snapshots" of activity on and between IT and OT systems (e.g., log files) • Workarounds/manual controls to physically isolate ICS networks to mitigate IT system risks for OT system processes	• Business justification and restrictive rules for all inbound/outbound access • Dial-up connectivity authentication • Use of an intermediate system for all interactive remote access • Methods to identify and terminate active vendor remote access sessions • Methods to identify and terminate authenticated vendor-initiated remote access connections for electronic access control or monitoring systems (EACMSs) and physical access control systems (PACSs)

	• Organization of OT system assets into logical zones, isolating unrelated subprocesses • Implementation of a DMZ, firewall rules, security architecture, and other tools to separate IT and OT system communication • Control local and remote access to Critical Cyber Systems • Define appropriate communication conduits between logical zones • Point-to-point encryption of OT system content when traversing IT systems • NIST SP 800-63 compliant multifactor access or other (compensating) logical and physical security controls for OT and IT access • Monitor, filter, and prevent unauthorized communication traffic between logical zones • Continuous data collection and analysis to identify potential intrusions and anomalous behavior • Network and/or system vulnerability identification and resolution • Document, audit, and investigate any communication between OT systems and any outside systems deviating from the identified communications baseline, ensuring it is necessary for operations • Biennial architecture reviews (network traffic verification/validation, system log reviews, and vulnerability analysis)	
Cyber System Physical Security [Physical Security, Visitor Access Management]	• Mitigation measures or manual controls to isolate ICSs when IT incidents create risks for OT system safety and reliability	• Physical Security Plan with operational and procedural controls • Allow only authorized unescorted access within the physical security perimeter (PSP) • Use at least two physical access controls for PSP access (where technically feasible) • Use a physical access point to monitor for unauthorized PSP access • Detect unauthorized PSP access and alarm/alert identified response personnel within 15 minutes • Monitor physical access control systems (PACSs) for unauthorized access • Detect unauthorized PACS access and alarm/alert identified response personnel within 15 minutes • Log physical PSP access (including date and time) • Retention of authorized PSP electronic access logs for 90 days • Access restrictions for cabling and non-programmable components outside the PSP but within the same PSP, issuing alarms/alerts to responsible personnel for communication failures within 15 minutes • PSP visitor entry logging • Continuous escorted visitor access within PSPs

		• Periodic maintenance and testing of PACS and PSP locally mounted hardware

System Security Management [Ports/Services, Patching, Malicious Code, Monitoring, Access Control]	• Monitor and/or block connections from known malicious command and control (CnC) servers to IP addresses and ports with unexpected external connections
	• Implement a patch management strategy to ensure all critical security patches/updates are current for Critical Cyber Systems
	• Categorize and determine patch/update criticality
	• Prioritize security patches/updates from CISA's Known Exploited Vulnerabilities Catalog
	• Develop and implement a patch/update implementation timeline based on categorization and criticality
	• Apply all IT patches/updates with a NIST score of "Critical" in CISA's Known Exploited Vulnerabilities Catalog within 15 days of availability
	• Apply all patches/updates for IT and OT operating systems, applications, drivers, and firmware
	• Install critical IT patches/updates that cannot be applied in the 15-day window within 30 days of listing in the Known Exploited Vulnerabilities Catalog
	• Install all non-critical IT system patches/updates within 30 days of availability
	• Install OT patches/updates for operating systems, applications, drivers, firmware, and software within 35 days of testing validation
	• If unable to install an IT patch/update for a "critical" vulnerability within 15 days, include it on a cumulative list with operational and other risk-based justification for not meeting the 15-day deadline
	• Maintain a cumulative list of critical OT patches/updates that cannot be installed within 35 days, including operational and other risk-based justification
	• Identify, prevent, block, and respond to unauthorized code execution (including macros)
	• Conduct weekly on-access and on-demand antivirus/anti-malware scans of IT systems, OT systems, and other network assets, using current signatures
	• Prevent malicious email traffic (e.g., SPAM/phishing)
	• Implement passive DNS capabilities consistent with currently recognized standards
	• List of frequently visited/searched domains (not already included in commercially available top one million domain lists)
		• Business justification for authorized logical ports and services
		• Deny all unnecessary access to physical input/output ports used for network connectivity, console, or removable media
		• Process to track release sources and to evaluate and install patches for "updateable" cyber assets
		• Evaluate all released patches within 35 days (TSA only requires OT patch/update testing)
		• Install all patches/updates within 35 days of testing
		• Create or update mitigation action plans (MAPs) or revise existing MAPs for patches/updates that cannot be applied within 35 calendar days of evaluation
		• Process to update signatures/patterns for malicious code detection methods (test and install)
		• BCS or cyber asset level logging to identify cyber security incidents:
		  ○ Successful and failed logins
		  ○ Failed logins
		  ○ Malicious code detection
		• Alerts for malicious code detection and event logging failure
		• Event log retention for 90 days
		• Periodic event log reviews to identify undetected cyber events
		• Authentication enforcement method for interactive user access
		• Identification / Inventory of Enabled Default or Generic Accounts (by the system, grouping, location, or system type)
		• Default Password Changes for Cyber Assets
		• Technical/procedural reinforcement of password-only authentication requirements:
		  ○ Length (lesser of eight characters or maximum supported)
		  ○ Complexity (lesser of three character types or maximum supported)
		• Limit the number of unsuccessful authentication attempts or generate alerts based on an attempt threshold

	• Policies/procedures to investigate the reputation of domains rarely queried and/or accessed by legitimate users, determining the risk level of communication with these domains • Use software analytics to determine which host sourced each DNS-query rapidly • Prevent users and devices from accessing malicious websites by implementing URL blocklists and/or allowlists • Control the impact of known/suspected malicious web domains and/or web applications • Audit unauthorized access to Internet domains and addresses • Implement signatures to detect and/or block connections from post-exploitation tools • Monitor and filter traffic between networks with different trust levels • Continuous monitoring policies/ procedures for critical systems to prevent, detect, and respond to cybersecurity threats and anomalies • Log OT systems/sites/environment "East-West" traffic (moving laterally within a trusted zone or LAN) • Log "North-South" traffic between IT and OT systems, and the perimeter boundaries between them • NIST-compliant log management and secure log management infrastructure • Develop, implement, review, and update NIST-compliant log retention policies and procedures • Implement a "Zero Trust" policy for IT and OT systems, providing layers of defense to prevent unauthorized execution • Implement separate dedicated Identity Providers for IT and OT systems • Review existing domain trust relationships and domain trust management to ensure necessity and adequacy • Remove all trust relationships, such as identity stores, between IT and OT systems • Limit shared accounts to those critical for operations, and only if absolutely necessary • Maintain a list of personnel who have or had access to group accounts • Change shared account passwords to prohibit access by individuals who no longer require access • NIST SP 800-63 compliant mandatory password resets for all IT systems (e.g., corporate remote access and VPNs) and all OT systems equipment (including PLCs) • Schedule periodic password resets • Maintain a list of dates for the last password resets • Maintain continuous compliance with all TSA-approved alternative measures	

	previously approved for systems where mandatory password resets are not technically feasible • Document MAPs for Critical Cyber System components without password resets and a timeframe to complete mitigation measures • Identify IT and OT systems equipment that does not permit NIST SP 800-63 compliant password resets, Develop and implement a timeline for equipment replacement, and submit for TSA approval	
Incident Reporting and Response Planning [Planning, Testing, Response, Handling]	• MAIN REQUIREMENT #2: • Incident Response Plan (IRP) to mitigate risks or operational disruption, or other significant impacts on necessary capacity during pipeline or facility incidents • Identify IRP responsibilities (by position) for implementing specific measures and any necessary resources needed for implementation • Implement advanced capabilities (e.g., SOAR) to define, prioritize, and drive standardized incident response activities • If SOAR is not applicable, document aspects of the system do not apply and provide justification for excluding these operations • Promptly Isolate and secure all infected and potentially infected devices and servers during an incident, clearly labeling any equipment affected by malicious code • Segregate (remove from the network) infected devices, along with any additional devices sharing a network with infected devices, to prevent malicious code from spreading • Preserve volatile memory by collecting a forensic memory image of the affected device(s) before powering off or moving	• Processes to identify, classify, and respond to cybersecurity incidents (CSIs) • Processes to evaluate and define attempted compromises, determine reporting applicability, and notify E-ISAC and NCCIC as required • Periodic IRP testing: ○ Reportable CSI ○ Paper drill/tabletop ○ Operational exercise • Use IRP to Respond to CSIs and document any deviations • Retain records reportable and attempted CSIs per IRP requirements • Following IRP testing or actual reportable CSI response (within 90 calendar days): • Document lessons learned or the absence thereof ○ Update IRP ○ Notify (individuals or groups) with IRP-defined roles • Changes to IRP roles, responsibilities (individuals or groups), or technologies (within 60 cal. days): • Update IRP • Notify (individuals or groups) with IRP-defined Roles • Initial CSI notifications and updates: ○ Functional impact ○ Attack vector ○ Attempted/achieved level of intrusion • Initial CSI Notification Timelines: ○ Within one hour of RCSI determination ○ End of the following calendar day for attempted compromise • Updates for new or changed attribute information (within seven calendar days)
Cyber System Recovery Plans [Business Continuity, Disaster Recovery]	• Implement governance capabilities to isolate IT and OT systems during actual (or potential) incidents that could result in operational disruption • Protect the security and integrity of data backups, including measures to secure and store them separately from IT and OT systems • Protect the security and integrity of data backups, including controls to secure and	• Conditions for recovery plan activation • Recovery responder Roles and Responsibilities • Processes for information backup and storage to recover BCS functionality • Processes to preserve data and to determine the cause of the CSI that resulted in plan activation • Periodic recovery plan testing: ○ Actual incident ○ Paper drill/tabletop

	store them separately from IT and OT systems • Ensure backup data is free of known malicious code during backup and when tested for restoral • Retain data for sufficient periods to allow effective investigation of cybersecurity incidents	○ Operational exercise simulating production environment • Periodic representative sample restoration (or actual recovery) • Periodic post-recovery plan test or actual recovery: ○ Document lessons learned or the absence thereof ○ Update recovery plan ○ Notify (individuals or groups) with recovery plan-defined roles • Changes to recovery plan roles, responsibilities (individuals or groups), or technologies (within 60 calendar days) ○ Update recovery plan ○ Notify (individuals or groups) with recovery plan-defined roles
Configuration Change Management and Vulnerability Assessments [Baselining, Change Management, Testing, Vulnerability Assessments, Transient Cyber Assets, Removable Media]	• Develop and implement router/switch configurations, including lists of publicly routable IP addresses and VLANs • Fully disable macros and user- based approval across the organization for Microsoft Office products (such as Word and Excel) using Group Policy • Determine exceptions on a case-by-case basis for macros required for business functionality • Only enable justified macros after implementing additional host-based security controls and network monitoring • Incorporate application allowlisting into system-change management • Update and review allowlists at least quarterly to remove applications no longer in use MAIN REQUIREMENT #3: • Develop and implement a TSA-approved Cybersecurity Assessment Program, including an annual performance plan • Within 60 days after TSA approval of TCIP, submit the annual assessment plan to TSA, including a specific assessment program actions schedule • Proactively and regularly assess cybersecurity measure (control) effectiveness • Perform penetration testing and “red/purple” team adversarial testing	• Baseline configuration (individual or group): ○ Operating system or firmware ○ COTS or open source (including version) ○ Custom software ○ Logical network ports ○ Applied security patches • Authorization and documentation of changes deviating from the baseline • Baseline configuration updates for completed changes deviating from baseline (within 30 calendar days) • Pre-change determination of change impacts: ○ Security controls ○ Adverse effects ○ Verification documentation • Test impacts of changes deviating from the baseline, documenting any differences between environments and the results: ○ In a test environment, or ○ Minimizing adverse effects in the production environment • Pre-change identification of software sources and the integrity of software obtained from those sources • Periodic baseline configuration change monitoring, documenting, and investigating unauthorized changes • Periodic paper or active vulnerability assessments • Perform testing in an environment that models the baseline or minimizes adverse effects in a production environment (documenting any differences between environments), and document testing results • Conduct active vulnerability assessments of new cyber assets before deployment to production (except for similar assets with a configuration modeling the existing baseline) • Document vulnerability assessment results and create MAPs with completion dates and execution status (remediation/mitigation)

		• Implement risk mitigation plans for transient cyber assets (managed by the entity or third party) and removable media
Information Protection [Information Protection, Reuse, Disposal]	• Implement 49 CFR Part 1520 protection for storing and transmitting documents (i.e., plans, reports, audit, testing, and assessment results)	• Method to identify BES Cyber System Information (BCSI) • Secure handling and protection for BCSI (in transit, during use, and stored at rest) • Proactive prevention of unauthorized BCSI retrieval from data storage media before releasing for reuse • Proactive prevention of unauthorized BCSI retrieval from cyber assets or data storage media before disposal
Communications between Control Centers		• Mitigation plan addressing potential unauthorized disclosure and modification of real-time assessment and real-time monitoring data transmitted between control centers • Identify where mitigating security controls are applied • Identify and delineate responsibility Between control centers operated by different entities

Supply Chain Risk Management [Planning, Procurement]		• Supply Chain Risk Management (SCRM) plan, including procurement planning processes
		• SCRM procurement processes:
		  ○ Notification by vendors of vendor-identified incidents
		  ○ Coordination of incident responses
		  ○ Notification by vendors when remote/or onsite access is no longer needed
		  ○ Vendor disclosure of known vulnerabilities
		  ○ Vendor software/patches integrity and authenticity verification
		  ○ Coordination of vendor-initiated remote access controls
		• Periodic SCRM plan review and CIP Senior Manager (or delegate) approval

Physical Security [Stations, Substations, Control Centers]		• Periodic physical security risk assessments for transmission stations, substations, and primary control centers • Unaffiliated third-party verification of physical security risk assessments

Table 3: Comparison of *TSA SD02C Mandated Pipeline Security Requirements to NERC CIP Standards*

Appendix E: Sample Compliance Challenges

Compliance Area	Compliance Challenge
Cyber System Categorization	•Proper asset categorization, classification, and inventory
Security Management Controls	• Developing robust compliance documentation (i.e., policies, plans, and processes)
Personnel & Training	• Implementing awareness campaigns and role-based cybersecurity training programs • Personnel risk assessment processes for employees and contractors (PRAs) • Human resources, attrition, and budgeting challenges
Electronic Security Perimeter(s)	• Creating proper segmentation using a zoned “zero trust” architecture, effectively separating IT systems from OT systems
Physical Security of BES Cyber Systems	• Robust layered physical security for IT and OT assets and systems
System Security Management	• OT asset and system compliance with the more IT-rooted technical NERC CIP standards and SD02-mandated requirements • Effectively mitigating risk from threat vectors, zero-day vulnerabilities, and other potentially exploitable weaknesses
Incident Reporting and Response Planning	•Incident handling and crisis communication management •Conducting “tabletop” and active response drills
Recovery Plans for BES Cyber Systems	•Business resiliency and continuity of operations planning •Crisis communications management
Configuration Change Management and Vulnerability Assessments	• Proper asset hardening and baselining (hardware and software) • Configuration and change management with formal approvals • Periodic cyber vulnerability and risk assessments
Information Protection	• BCSI protection during transit, during use, and at rest during storage • Cyber asset preparation for reuse and/or disposal
Communications between Control Centers	• Real-time monitoring of control center communications
Supply Chain Risk Management	• Supply chain risk management planning and execution • Effective contract and service level agreement (SLA) wording
Station and Substation Physical Security	• Independent third-party validation of station/substation physical security risk assessments

Table 4: *Sample NERC and TSA Compliance Challenges*

About ITEGRITI

Companies often struggle with ongoing operational, cybersecurity, and cybersecurity compliance responsibilities. While it is tough to recruit, train and retain quality talent, it can be even harder to find highly qualified and dependable consultants.

ITEGRITI has assisted Critical Infrastructure organizations across the U.S. and Canada with IT and OT cybersecurity and compliance since 2008.

Our team has deep expertise gained through our work in protecting large-scale and distributed National Critical Infrastructure since compliance with the cybersecurity Standards first became mandatory. We are flexible, will easily integrate with your team, bring relevant best practices and lessons learned, and will deliver tangible results.

Contact Us

ITEGRITI Corporate Office
2101 CityWest Boulevard
Suite 100
Houston, TX 77024
Phone: +1 832.781.3001

Southeast Regional Office
101 N Tryon Street
Suite 112
Charlotte, NC 28246
Phone: +1 704.457.9641

itegriti.com/contact
info@itegriti.com

Our Purpose
To help protect National Critical Infrastructure

Our Mission
To develop, implement, and support cybersecurity and compliance programs that help clients reduce risk and defend National Critical Infrastructure against cybersecurity threats.

Our Values
We are a values-driven organization. The name "**ITEGRITI**" is an intentional variation of the word "integrity," which is not only what we bring to the cyber environments of our clients but how we go about performing our work – with integrity.

About The Author

Dr. Thomas "Tom" Duffey, Director Cybersecurity and Compliance
(CISSP, CISM, CISA, C|CISO, CGRC, CDPSE, C|EH, CCNP-S, FITSP-M, GCIP, MCSE, PMP)

Dr. Tom specializes in critical infrastructure cybersecurity and regulatory compliance for the defense, healthcare, and energy (utilities and oil & gas) sectors. He brings over 30 years of experience to the table and is passionate about protecting operational technology (OT) and the Internet of Things (IoT) for various industries. Tom's diverse consulting, training, and project management experience also includes supporting multiple military branches (U.S. Army, Navy, Air Force, Marines, Army Reserve, and Air National Guard) at numerous CONUS and OCONUS facilities across the globe.

Tom resides in Houston, TX, where he leads OT/IT/IoT critical infrastructure protection delivery efforts for multiple ITEGRITI clients and is part of the local FBI InfraGard leadership team. Teaching and learning are two of Tom's biggest passions. Along with contributions to numerous security thought leadership efforts, including a World Economic Forum whitepaper and the EC-Council C|CISO Body of Knowledge, Tom earned his Doctoral degree in Computer and Information Security. His dissertation explores the Impact of NERC CIP regulatory compliance on security and risk.