THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

NSTAC REPORT TO THE PRESIDENT

Information Technology and Operational Technology Convergence

August 23, 2022

Contents

Figures

Tables

Executive Summary

In May 2021, in the aftermath of a series of significant cybersecurity incidents, the White House tasked the President's National Security Telecommunications Advisory Committee (NSTAC) with conducting a multi-phase study on "Enhancing Internet Resilience in 2021 and Beyond." The tasking directed NSTAC to focus on three key cybersecurity issues foundational to United States (U.S.) national security and emergency preparedness (NS/EP):

1. Software Assurance in the Commercial Information and Communications Technology Supply Chain.
2. Zero Trust and Trusted Identity Management.
3. The Convergence of Information Technology (IT) and Operational Technology (OT).

The first three phases of the tasking focus on developing recommendations to address each of these issues. The fourth phase will refine and build upon the key findings of phases I, II, and III to produce an overarching report.

This report focuses on the third issue, the convergence of IT and OT.

Introduction

IT/OT convergence refers to the connection of formerly isolated OT systems, (e.g., electrical substations, water treatment plants, and manufacturing facilities) to the Internet, either directly or through various enterprise network pathways. Common IT devices and systems, such as routers, servers, switches, and cloud computing applications, are also increasingly combined with OT applications. This combination makes OT systems susceptible to the same risks of malware and threats that IT systems face today.

IT systems and OT systems are different in many ways. First, OT systems have differing performance requirements than IT systems, which creates a challenge when applying IT security to OT systems. Second, IT systems are designed for general use, and these systems support a wide variety of technologies, applications, and users. Conversely, OT systems serve a specific purpose, and these systems therefore focus on specific requirements and perform a specific function. Finally, the expected lifecycle of an OT system is a decade or longer, which is a much longer lifecycle than that of an IT system. This creates different priorities between IT security professionals and OT system operators within organizations. While IT security practices can inform OT security requirements, the OT systems require more specialized solutions which address the performance requirements of the systems.

It is difficult to maintain the security of these OT environments over time via a traditional IT approach (such as patching), and in some cases the acceptable timeline to resolve issues is much different. Many OT environments still utilize legacy technologies that are decades old. Organizations have intentionally interconnected these systems over past years to access data, which can help drive decisions to gain a competitive advantage, and to drive operational efficiencies, such as predictive maintenance, remote monitoring, and just-in-time manufacturing. However, these organizations often did not conduct an evaluation of the risk that was being

introduced, the potential consequences to the business, and the implications for NS/EP prior to connecting the systems.

As IT and OT convergence accelerates, an increasing number of cyber-attacks will continue to traverse the boundaries of IT and OT for a few reasons. First, many organizations claim to have employed an architecture for OT systems that include an "air gap", whereby IT and OT systems are completely isolated from each other. This "air gap" is rarely found when doing IT/OT risk assessments. Unless there are strict internal controls and organizational discipline to enforce them, there will be natural human instinct to work around inefficiencies. Second, many systems can even "accidentally converge," where the system owner does not even realize or have visibility into which devices reside where on their networks. Finally, the existence of "Shadow IT," where systems are added and modified without official IT change management control and approval in the OT domain, is quite real.

In early February of 2022, NSTAC began developing this report to examine the key challenges of securing OT systems against threats that emerge from IT network connections; and to identify emerging approaches to increase OT resiliency to these threats, including through adaptations of IT security approaches to accommodate OT design constraints. Shortly afterward, Russia launched its invasion of Ukraine, fundamentally changing the security environment in both the physical and cyber realms and significantly raising the importance and relevance of the Enhancing Internet Resilience study. Critical infrastructure in our country faces a pointedly heightened threat landscape, which elevates the importance of securing IT and OT systems, including those in converged IT/OT environments.

Critical infrastructure increasingly relies on converged IT and OT systems to operate. A compromise of these systems could lead to disruptions of service or critical processes, resulting in significant cascading impacts throughout U.S. critical infrastructure and beyond. Because OT systems control physical assets, system failures can pose significant safety risks for organizations' employees and customers. These risks heighten the importance of thoughtfully and effectively managing IT/OT convergence. Government and industry must navigate through this OT risk landscape to deliver the essential products and services that support societal well-being and fuel the economy.

Report Focus and Scope

In July 2021, the administration issued the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems[1], outlining initiatives in the electricity, pipeline, water, and chemical sectors, and calling for the development of cross-sector cybersecurity performance goals for critical infrastructure.

For the purposes of this report, NSTAC focused specifically on the convergence of IT/OT for government departments and agencies as well as industrial or critical infrastructures. The report aims to identify

[1] The White House, "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems," July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

opportunities for the federal government to aid in a secure convergence of OT cybersecurity within all relevant stakeholder communities.

To inform its study, NSTAC conducted outreach and sent formal invitations to three different sets of stakeholders over three phases. In the first phase, NSTAC requested briefings from government-related entities and sector risk management agencies with roles in IT/OT convergence. These entities' roles include enacting policy changes to improve IT/OT security, and operating government IT/OT infrastructure. Briefers included representatives from the National Security Council (NSC), the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Defense (DoD), the Department of Energy, the Federal Energy Regulatory Commission, the Federal Bureau of Investigation, and the Department of Transportation. In the second phase, NSTAC requested briefings from asset owners and operators of IT/OT infrastructure, and original equipment manufacturers in the chemical, energy, transportation, water/wastewater, logistics, communications, and cloud service provider industries. Finally, in the third phase, NSTAC hosted briefings by representatives from the vendor/supplier/integrator community that provide cybersecurity products and services in the IT/OT convergence space.

Summary of Key Findings

Several consistent themes and findings have emerged from the experts that have briefed NSTAC:

- The cybersecurity challenge of converged IT and OT is not a new issue; it has been happening for decades. The United States has the technology and the knowledge to secure these systems but has not prioritized the resources required to implement solutions.

- In contrast to IT cybersecurity attacks, the outcomes of successful OT attacks include the potential to impact human safety and damage physical equipment, taking any industrial processes OT equipment supports offline for extended time periods.

- The United States can leverage an existing body of knowledge to secure OT infrastructure. Prioritizing and applying these best practices, recommendations, and standards more broadly, in a comprehensive and accelerated manner, would strengthen security and achieve strategic outcomes.

- Many organizations lack visibility into their complete OT environments, including IT/OT interconnections and supply chain dependencies. They also lack clear direction from the government on what level of threat that they should be protecting against, and as a result there is confusion about the appropriate level of cybersecurity required to combat threats.

- Cybersecurity is overwhelming for organizations and entities with small staffs and budgets. As a result, many are not able to achieve the cybersecurity posture required to adequately secure their IT/OT infrastructure.

- Some legacy OT equipment was never designed for internet connectivity, and may not easily be replaced, making it increasingly challenging to secure in converged environments.

- It is imperative to break down silos which exist between personnel in the IT and OT teams within organizations and bring them into a more unified structure to more effectively manage the shared responsibility to secure converged environments.

- Stakeholders rarely take the opportunity to proactively "build in" security where appropriate and opt instead to "bolt on" security in OT environments after the fact.

- Cybersecurity is rarely required in public and private sector OT requests for proposals and procurement processes.

- While government regulations may be necessary in certain instances to help improve infrastructure security, these regulations should be flexible, outcomes-oriented, standards-based, vendor agnostic, and should promote interoperability.

- Cybersecurity education and ease of access to training for the critical infrastructure workforce is lacking, however it is an essential element to improving long-term industrial security.

Summary of Recommendations

During this study, NSTAC heard from experts from multiple companies, organizations, and stakeholders regarding the challenges they face around IT/OT convergence. Significant work remains to incorporate and secure these highly diverse and heterogeneous OT systems. The implications of converging these systems with IT are poorly understood.

The technology to implement basic cybersecurity fundamentals to secure these systems exists in the commercial market. The talent to understand how to secure the systems also exists, albeit not at the necessary scale, to implement the security requirements broadly for critical infrastructure.

The biggest gap is that end users, including federal government owners and operators, have not prioritized resources to address the cybersecurity of these systems and networks at the appropriate levels. Government agency heads and business leaders face extremely difficult budgeting decisions. However, there needs to be a stronger understanding of the relationship between cybersecurity for converging OT systems and organizational mission and risk, especially as OT systems often operate an organization's "crown jewels." While cybersecurity of IT systems is often characterized in terms of confidentiality, integrity, and availability, the cybersecurity of OT systems prioritizes safety and reliability. The loss of functionality of an OT system can have dire safety consequences.

Many of these recommendations are not new and the authors of prior reports have discussed and proposed them. The technologies, processes, and procedures exist to secure the convergence of the IT and OT domains. The major impediment to securing IT/OT convergence and protecting the nation's critical infrastructure is the lack of urgency to make the necessary investments and required changes. The time for action is now.

With that in mind, NSTAC has prioritized the following critically important recommendations for the president to implement, which would provide immediate improvement for the cybersecurity posture of United States government (USG)-owned and operated OT systems, with relatively low risk.

Asset Management for USG-owned OT	***Require inventory of USG OT Systems and hold agencies accountable.*** *CISA should issue a Binding Operational Directive (BOD), similar to what Section 1505 of the Fiscal Year 2022 National Defense Authorization Act[2] requires for the DoD, that requires executive civilian branch departments and agencies to maintain a real-time, continuous inventory of all OT devices, software, systems, and assets within their area of responsibility, including an understanding of any interconnectivity to other systems. An up-to-date inventory should be required as part of each department or agency's annual budget process. Once federal agencies clearly understand the vast and interconnected nature of their OT devices and infrastructure, they can then make risk-informed decisions about how to prioritize their cybersecurity budgets to best protect the most consequential of those assets. The White House should mandate periodic reports from CISA on department and agency implementation of this BOD to ensure progress is made.*
Procurement Language	***Develop enhanced OT-specific cybersecurity procurement language and ensure all USG OT procurements include cybersecurity provisions.*** *CISA should develop guidance on procurement language for OT products and services, and for products and services that support converged IT/OT environments, to incentivize the inclusion of risk-informed cybersecurity capabilities, including for supply chain risk management; this guidance should also help organizations understand best practices for bolt-on security for legacy OT devices that are difficult or expensive to replace.* *CISA should work with the General Services Administration to require the inclusion of risk-informed cybersecurity capabilities in procurement vehicles for the federal government.* *There should also be a mechanism for both private sector consumers of the procurement guidance and public sector agencies, which must follow the new requirements, to provide feedback and lessons learned to aid the community.*

[2] United States (U.S.) Congress, National Defense Authorization Act for Fiscal Year 2022, December 27, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1605/text.

Communications and Information Sharing	***Standardize and enable real time interoperable information sharing (Beginning with USG-owned environments).*** *The NSC, CISA, and the Office of the National Cybersecurity Director should prioritize the development and implementation of interoperable, technology-neutral, vendor-agnostic information sharing mechanisms to enable the real time sharing of sensitive collective-defense information between authorized stakeholders involved with securing U.S. critical infrastructure. This should include breaking down the artificial barriers for sharing controlled unclassified information, both within the USG and between the USG and other key, cross-sector stakeholders.*

While no less important, the remaining list of recommendations should be considered and will require more interagency discussion and collaboration and require a longer timeline to achieve the desired results.

Category	Recommendation
USG Roles, Responsibilities and Accountabilities	***Articulate federal roles, responsibilities, authorities, and accountabilities.***
Communications and Information Sharing	***Streamline stakeholder communications with USG cyber defenders.***
National OT test beds / System Integrators and Cloud Service Providers	***Catalog and further develop physical and virtual OT security test beds.***
Zero Trust	***Extend existing federal zero trust guidance into OT where applicable.***
State, Local, Tribal, and Territorial (SLTT)	***Ensure OT cybersecurity projects are funded in Infrastructure Investment and Jobs Act (IIJA) implementation.***
SLTT	***Expand CISA services into OT specifically for SLTT critical infrastructure.***
Regulated Sectors	***Ensure adequate IIJA Energy Title funding is dedicated to OT cybersecurity projects.***
Regulated Sectors	***Identify opportunities to streamline OT cybersecurity regulation.***

Category	Recommendation
Non-Regulated Sectors	*Promulgate lessons learned from regulated sectors.*
Public, Private Partnerships	*Designate a lead cross-sector OT cybersecurity partnership effort.*
People and Workforce	*Catalog and assess efficacy of OT workforce development efforts.*
International collaboration	*Ensure international efforts in cybersecurity include OT.*

NSTAC's goal for this report is to provide the president with strategic and immediately actionable recommendations that the federal government should implement to further reduce risk and secure the nation's critical infrastructure. NSTAC also recognizes that the federal government alone cannot uniquely resolve all the challenges surrounding OT cybersecurity, and readers from all stakeholder groups will benefit from the additional findings, best practices, and general guidance contained in the appendices.

1. Stakeholder Perspectives

1.1. Federal Government Perspectives

1.1.1. Asset Management for Federally Owned and Operated Operational Technology (OT) Systems

One of the recurring themes in briefings and discussions hosted by the President's National Security Telecommunications Advisory Committee (NSTAC) was that federal and private sector organizations have limited visibility into what OT assets they own and operate and how those systems and devices are interconnected with enterprise or other networks. Fortunately, technologies exist to allow end users to perform asset inventory assessments of OT systems. Agency heads need to deploy those technologies in a disciplined process to gain full visibility into the scope of their OT environment.

Executive Order (EO) 14028 (EO 14028), *Improving the Nation's Cybersecurity*, released in May 2021, states that "the federal government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems…" In addition, it states that "the scope of protection and security must include systems that process data (information technology [IT]) and those that run the vital machinery that ensures our safety (OT)."[3]

EO 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, released in May 2017, states that federal agency heads will be held accountable by the president for "implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data".[4]

Further, there is an opportunity to leverage the accountability included in EO 13800 with the expanded scope of protection and security to include OT systems in EO 14028.

Recommendation: Require inventory of United States Government (USG) OT Systems and hold agencies accountable.

The Cybersecurity and Infrastructure Security Agency (CISA) should issue a Binding Operational Directive (BOD) requiring executive civilian branch departments and agencies to maintain a real-time, continuous inventory of all OT devices, software, systems, and assets within their area of responsibility, including an understanding of any interconnectivity to other systems. An up-to-date inventory should be required as part of each department or agency's annual budget process. Once federal agencies clearly understand the vast and interconnected nature of their OT devices and infrastructure, they can then make risk-informed decisions about how to prioritize their

[3] The White House, "Executive Order (EO) 14028: Improving the Nation's Cybersecurity," May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[4] The White House, "EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

cybersecurity budgets to best protect the most consequential of those assets. The White House should mandate periodic reports from CISA on department and agency implementation of this BOD to ensure progress is made.

Agency head accountability for protection of IT systems and data should be extended to include protection of OT systems that are owned and operated by USG departments and agencies.

1.1.2. Procurement Reform and Standardized Procurement Language

One of the consistent themes that suppliers, vendors, end-users, and cloud service providers and integrators briefed to NSTAC was that cybersecurity controls in OT environments are still neither universally requested nor required in procurement contracts. Original Equipment Manufacturers (OEM) and vendors state that they stand ready to deliver additional security features, products, and services, but their customers are not requesting these options. This may stem, in part, from the user's lack of knowledge of available options. Others have stated that in many industries, such as electrical and/or water, where rate controls may be in effect and where customer cost tolerance is a significant issue, the practice of selecting the lowest-cost bid still prohibits the inclusion of cybersecurity requirements not mandated by law.

Relatively few OT system operators have the expertise and workforce to plan and deliver IT/OT convergence projects themselves. As a result, a large ecosystem of systems integrators (SIs) supports operators with technology services across a broad range of domain expertise. In some cases, these SIs are long-term partners with the operators and remain involved in the day-to-day maintenance and running of the systems they have delivered. However, it is more common for their engagements to be fixed-length capital projects, at the end of which the operator is left to run and maintain the system with their existing staff. This poses a challenge to the ongoing operational nature of cybersecurity.

Most operators have commercial or regulatory needs to select the lowest cost bidder when considering proposals from SIs. As a result, integrators are disincentivized from adding scope to proposals where cybersecurity requirements are not explicitly included in the operator's requests for proposals. Operators in segments such as public utilities, where associated regulation is intended to ensure appropriate use of public funds, may explicitly prevent vendors from adding additional requirements beyond the functional requirements of the project. As a result, SIs rely on their customers to specifically request those services as part of the procurement process.

Operators and integrators are increasingly aware that the project bidding and planning process is one of the key constraints on achieving their mutual cybersecurity goals, but there is little consensus on how to solve it in a way that supports competitive bidding. Unlike functional requirements where it is relatively easy to compare bids and competitive offers, there is not yet a clear way to communicate expectations and outcomes around cybersecurity. As a result, integrators struggle to articulate a clear value proposition and operators struggle to understand whether the proposals are a good use of money or will meet their cybersecurity goals. The more sophisticated operators and integrators can navigate this uncertainty by relying on their skilled workforce to carefully evaluate proposals, but this process is imprecise, expensive, and not always within reach for all operators of critical infrastructure. All parties involved in these transactions would benefit from a more concrete way to communicate, evaluate, and compare cybersecurity service offerings.

The United States (U.S.) Department of Homeland Security (DHS), in conjunction with the U.S. Department of Energy (DOE) and the SANS Institute, first released a procurement language guide for industrial control systems security in 2009.[5] A collaborative multi-agency, government-sponsored initiative to update this guidance, along with an education and enablement campaign to incentivize its use, would have great value. The federal government should lead by example and ensure that all federal procurements of OT systems and services include OT cybersecurity provisions.

Recommendation: Develop enhanced OT specific cybersecurity procurement language and ensure all USG OT procurements include cybersecurity provisions.

CISA should develop guidance on updating and enhancing IT/OT products and services procurement language to incentivize the inclusion of risk-informed cybersecurity capabilities within delivered products and services; this guidance should also help all organizations understand best practices for bolt-on security for OT devices that are much more difficult or expensive to replace.

CISA should work with the General Services Administration to require the inclusion of risk-informed cybersecurity capabilities in procurement vehicles for the federal government. In the development of these requirements, CISA should review new federal agency and department cybersecurity requirements under EO 14028, including software assurance and zero trust architecture requirements, for applicability in OT environments and include these where appropriate.[6]

There should also be a mechanism for both private sector consumers of the procurement guidance and public sector agencies, which must follow the new requirements, to provide feedback and lessons learned to improve the procurement language.

1.1.3. Communications and Information Sharing

Open and transparent information sharing should be the default approach inside of the U.S. federal government. There are many reasons this hasn't historically been the case, such as the lack of alignment among Sector Risk Management Agencies (SRMAs) with oversight from different congressional committees, legacy missions, competition for limited budgets, etc. These challenges are further exacerbated by incompatibility between various controlled unclassified information (CUI) designations used by departments and agencies. For example, DHS and CISA use the term "protected critical infrastructure information," also known as PCII[7], the Transportation Security Administration which, while also part of DHS, uses the term "sensitive security

[5] Department of Homeland Security (DHS), "DHS: Cyber Security Procurement Language for Control Systems," September 2009, https://us-cert.cisa.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf.

[6] The White House, "EO 14028: Improving the Nation's Cybersecurity".

[7] "Protected Critical Infrastructure Information Program," Cybersecurity and Infrastructure Security Agency (CISA), accessed July 13, 2022, https://www.cisa.gov/pcii-program.

information" or SSI[8], and DOE uses "critical electric infrastructure information" or CEII[9]. Each of these information sharing programs stem from different legal requirements and legislation, have different protection requirements, and exist in different systems and databases. Employees of different federal agencies cannot easily share information with one another, even those holding top-secret security clearances. It is easier to share highly classified and compartmentalized intelligence about an adversary's infrastructure internally than it is to share information about our own critical infrastructure between two U.S. government agencies.

Various government departments and agencies are competing for jurisdiction and funding from Congress. An important example of this is for "cybersecurity sensors" within critical infrastructure sectors. CISA has a variety of mature capabilities that have been in place within federal government departments and agencies for several years, and they are pivoting to apply them to private sector or State, Local, Tribal, and Territorial (SLTT) applications (Einstein, Albert, CyberSentry, etc.) and SRMAs. DOE also has significant and mature capabilities that have been deployed within their sectors for several years, including the Cybersecurity Risk Information Sharing Program, otherwise known as CRISP. Cybersecurity solution providers have advocated for vendor agnostic, technology neutral, interoperable, standards-based approaches to sharing situational awareness data to protect critical infrastructure. The U.S. government should do the same.

Recommendation: Standardize and enable real time interoperable information sharing.

The National Security Council (NSC), CISA, and the Office of the National Cybersecurity Director (ONCD) should prioritize developing and implementing interoperable, technology-neutral, vendor-agnostic information sharing mechanisms to enable the real-time sharing of sensitive collective-defense information between authorized stakeholders involved with securing U.S. critical infrastructure. This should include breaking down the artificial barriers for sharing CUI both within the U.S. federal government and between the federal government and other key, cross-sector stakeholders.

In conjunction with this development and implementation, the federal government should retire the existing morass of information-sharing portals, systems, and mechanisms that exist under a patchwork of policy and law. If the government can truly streamline and optimize these mechanisms for collaboration, the impact would be enormous.

1.1.4. Roles and Responsibilities

NSTAC learned that confusion remains about whom specifically to engage within the federal government when there is a cybersecurity incident or question. Stakeholders face duplicative reporting requirements to local, state, and/or federal agencies, each with different reporting formats and deadlines. This challenge seems to be especially compounded with OT and Industrial Control Systems (ICS). The Federal Bureau of Investigation (FBI)

---

[8] "Sensitive Security Information," Transportation Security Agency, accessed July 13, 2022, https://www.tsa.gov/for-industry/sensitive-security-information.

[9] U.S. Department of Energy (DOE) Office of Electricity, "Critical Electric Infrastructure Information Final Rule: Questions and Answers," May 15, 2020, https://www.energy.gov/oe/articles/critical-electric-infrastructure-information-final-rule-questions-and-answers.

has long-standing local presence in most American cities and has made a concerted effort to establish and expand relationships with American businesses regarding cybersecurity. CISA is also establishing local and regional presence with their cybersecurity advisors. SRMAs, and in some cases regulators, also have a desire to interact with individual companies or entities, leaving smaller organizations somewhat overwhelmed.

Recommendation: Articulate federal roles, responsibilities, authorities, and accountabilities.

CISA, the ONCD, and the NSC should clearly articulate the respective roles and responsibilities for the various executive branch departments and agencies that provide support to stakeholders across critical infrastructure and other sectors. This should also specifically include what actions departments and agencies should not take to avoid duplication.

The Office of Management and Budget (OMB) should work with CISA to develop key IT/OT convergence cybersecurity performance indicators and implementation timelines. Once those are in place, OMB should hold agency heads accountable for achieving these indicators and timelines and use those performance indicators and implementation times to drive annual cybersecurity budget development.

Various structures within DHS have attempted to streamline cybersecurity communications. Examples include the National Cybersecurity Communications Integration Center, or "CISA Central" as it is now called. However, these structures are not cross functional and law enforcement, SRMAs, and regulators remain siloed. In the U.S., if individuals have an emergency, they dial 911 on their telephone and the dispatcher will provide initial triage and route their call based on the nature of the emergency. For organizations that are facing cybersecurity attacks, there is not an equivalent service. For the federal government to lead in this area, it needs to make crystal clear the roles and responsibilities, authorities, and accountability requirements for all agencies involved, and make access to those products, services, and people as simple as dialing 911. This service should be a dispatch function, where organizations are asked, "what is your emergency?" and are routed to the correct department or agency to be connected to the appropriate cyber defender. This would solve two problems: (1) there would be a single point of contact for all critical infrastructure operators; and (2) DHS would be alerted to all incidents, even if the case was subsequently transferred to a different SRMA.

Recommendation: Streamline stakeholder communications with USG cyber defenders.

The ONCD, CISA, and the FBI should streamline and simplify the mechanism for all cybersecurity stakeholders (federal department and agency, state local tribal or territorial agency, private company, individual citizen, and international partner) to quickly connect with the right person within the federal government to address their cybersecurity concern. The newly passed cybersecurity incident reporting legislation, which was included in the Fiscal Year 2022 Omnibus Appropriations bill[10], provides the legislative authority and mechanism through which this should be achieved. ONCD, CISA and the FBI should leverage work on emergency response that the National

[10] U.S. Congress, Public Law 117–103: Making Consolidated Appropriations for the Fiscal Year Ending September 30, 2022, and for Providing Emergency Assistance for the Situation in Ukraine, and for Other Purposes, March 15, 2022, https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf.

Institute of Standards and Technology (NIST) has developed in partnership with industry, such as the Framework for Cyber-Physical Systems[11], as well as emergency response guidance in industry-driven standards, such as the International Society for Automation/International Electrotechnical Commission 62443 body of standards[12]. The goal should be to make this as easy as dialing 911.

1.1.5. National Cybersecurity OT Test Beds

Approximately a decade ago, specialized, or custom purpose-built cybersecurity technology capable of operating within critical infrastructure OT networks was scarce, had limited capabilities, or simply did not exist. Through investment in research and development by governments, academia, and the private-sector, technologies are now maturing that enable continuous monitoring, inspection, threat detection, and other security capabilities within these environments. Regardless, organizations find it difficult to select, test, install, and validate these solutions to meet their risk mitigation objectives.

Every organization has a different tolerance for risk, and each system we are protecting may need a slightly different approach to cybersecurity. However, we cannot afford to wait and go through the iterative trial and error process, as we did with enterprise security, to allow the natural selection of these technologies to occur. We must find ways to accelerate this decision-making and deployment process so that end users can quickly get comfortable with their choice of cybersecurity solutions.

In some areas, the standards used for certain critical infrastructure sectors do not allow the use of cloud services. However, in those sectors which permit them, and with the rapid rise of cloud services technology in IT, cloud service providers (CSPs) are becoming stakeholders in IT/OT convergence projects. There is considerable variance and experimentation in how the integrators and the CSPs interact within these projects. In some cases, the CSP is simply a vendor to the integrators with little involvement in the design or delivery of the project, and, in some cases, they coordinate closely as partners. In other cases, the CSPs' professional services arms are themselves acting as the integrators.

Increasing adoption of cloud services presents both opportunities and risks for cybersecurity of IT/OT converged projects. Cloud services and their "software-defined infrastructure" approach support cybersecurity practices like asset inventory and configuration management and can accelerate threat detection and response by the central remote management that cloud services provide. However, much of the existing security guidance for OT systems relies on network isolation to protect critical equipment from outside threats.

Introducing internet-delivered services into these systems requires careful adaptation of existing controls, increasing the complexity of the network configuration, and introducing risk of accidental network exposure of assets which were meant to be isolated. As a result, many CSPs are supportive of progress towards Zero Trust

---

[11] National Institute of Standards and Technology (NIST), Special Publication (SP) 1500-201, "Framework for Cyber-Physical Systems": Volume 1, Overview, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf.

[12] "International Society of Automation (ISA)/International Electrotechnical Commission (IEC) 62443 Series of Standards: The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards," ISA, accessed July 13, 2022, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

Architectures (ZTA), which will reduce reliance on network isolation in favor of more explicit security controls that are designed for use over potentially hostile networks. However, even advanced architectures like ZTA cannot resolve fundamental availability risks of services delivered over the internet, where disruptions of physical networking infrastructure or denial of service attacks can interfere with service delivery. As a result, IT/OT projects that rely on cloud services need to be designed and tested to ensure they continue to provide their essential functions when internet connectivity is disrupted.

The technology and architectural practices to support this need are still immature but developing rapidly. Some standards and regulatory frameworks, notably International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443, are currently being updated to describe the roles and responsibilities of the various stakeholders in IT/OT systems that incorporate cloud services.[13] However, many existing regulations and security frameworks are still written in a way that precludes or significantly complicates integration of cloud services.

When any new hardware or software technology is introduced to an OT environment, or when a patch is applied, it needs to be thoroughly tested to ensure interoperability with the current production environment. Further, organizations need the ability to practice recovery from system attacks and failure. Complicating this process are the many additional features and applications that may be found in IT equipment, but that are not desirable in OT environments. Combining this complexity with cybersecurity needs, the integration of OT equipment creates significant challenges for organizational testing teams.

Recommendation: Catalog and further develop physical and virtual OT security test beds.

CISA and the SRMAs should work with academia and private industry organizations to catalog existing centers, and to fund, and further develop both physical and virtual testbed style centers, specifically including cloud-based technologies where applicable. This will enable organizations to test drive and validate various technology configurations, including those that incorporate cloud services, in an environment representative of their particular sector. These test beds also enable simulation of impactful events and allow for exercising and testing recovery procedures. IT security architecture approaches, such as the separation of events from data and management planes, can be evaluated for their efficacy in the OT domain.

CISA should maintain a central repository for testing results. This will allow anyone implementing the technology to better understand equipment and how it interacts with their environment.

These types of testbed facilities exist in certain sectors, including those sponsored by DOE and other departments and agencies, as well as the private sector, but the U.S. lacks critical mass. Government investment in this area would prove valuable beyond the technology selection considerations. For example, the facilities could be used to train all types of personnel required to secure the systems and exercise incident response capabilities between government and industry.

---

[13] ISA/IEC 62443 Series of Standards: The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards".

1.1.6. Zero Trust in OT Environments

Section 3 of EO 14028 specifically calls for federal agencies and their suppliers "to modernize [their] approach to cybersecurity" by accelerating the move to secure cloud services and implementing a ZTA[14]. ZTA is a cybersecurity strategy and is not a technology that an organization can purchase. While ZTA may raise the bar for cybersecurity, it can be extremely difficult to implement in OT environments, which include both legacy equipment and new equipment. Much of the legacy and new ICS equipment does not meet the requirements to implement the zero trust controls.

However, as more OT systems converge with IT systems, such as cloud applications, it becomes important to audit internet-facing assets to determine any underlying risks. Organizations can hire an external party to assess the risk with their internet-facing assets, or they can utilize external attack surface management tools to automate the process as part of their security programs.

As with on-premises OT environments, a key first step in implementing ZTA is to define the "protect surface" (data, assets, applications, and services) then implement the policies and control infrastructure. Unlike most on-premises OT environments, today's cloud security technologies in fact support the micro-segmentation of cloud assets at the virtual machines, containers, applications and serverless systems. Role-based access control is also possible via cloud-based identity and access management solutions. Of particular concern are conduits/policies which allow remote access/control over OT systems. These policies should be closely scrutinized by IT and OT teams and be restricted to mission critical purposes following appropriate risk-benefit analysis.

Recommendation: Extend existing federal zero trust guidance into OT where applicable.

Following the recommendations in the NSTAC Report to the President on Zero Trust and Trusted Identity Management,[15] the subcommittee recommends that OMB should undertake a comprehensive process to identify OT systems and services across federal agencies. Once identified CISA and appropriate SRMAs should establish an interagency working group to create corresponding OT-specific Zero Trust Maturity Models where applicable for how to protect each service, modeled after the Zero Trust Maturity Model use case NSTAC created for Directory Services.[16]

ZTA should not be an all or nothing implementation for an OT environment because some existing and some new equipment will not meet the requirements for ZTA controls. As a result, any created Zero Trust Model should consider a hybrid approach of traditional best practices wrapped by ZTA.

---

[14] The White House, "EO 14028: Improving the Nation's Cybersecurity".

[15] President's National Security Telecommunications Advisory Committee (NSTAC), "Report to the President on Zero Trust and Trusted Identity Management," February 2022, https://www.cisa.gov/nstac-publications.

[16] "Zero Trust Maturity Model," CISA, accessed August 3, 2022, https://www.cisa.gov/zero-trust-maturity-model.

1.2. State, Local, Tribal, and Territorial Government Perspectives

SLTT governments are responsible for overseeing safe, reliable, economical, and environmentally friendly services to the public under their jurisdiction. Some of these services, such as water and wastewater or electric utilities, are owned and operated by their respective government while others are owned and operated by a private utility but regulated by the government.[17]

The overseeing government entity regulates the utility to ensure safety and, in some instances, such as electric, regulates the rates to the customer that are based on reasonable and expected utility expenses. These expenses may include capital investment for cyber infrastructure and operating expenses. Regardless of the oversight, a utility will carefully consider costs associated with infrastructure upgrades or modifications, because the costs may not easily be passed to the consumer. These costs also include improving the cybersecurity of the system but not necessarily improving the efficiencies.

The need for cybersecurity exacerbates the complexity of these systems converging. The technology changes at a pace that staff may have difficulty keeping up with, especially for smaller organizations. This is evident by the fact that most vendors who briefed NSTAC discussed that many customers of OT systems are not aware of available cybersecurity options. Most integrators of the technology also expressed that the volumes of standards and guidance that exist make it difficult and often overwhelming to adhere and/or comply. Procurement reform guidance, as called out previously in Recommendation 1.1.5, can help to alleviate these concerns.

Many SLTT utilities cover large geographical areas with small budgets that are used to implement and maintain the OT systems. As these systems converge and become more complex, the technology lifecycle is shortening, requiring more frequent changes. These changes require higher budgets and knowledgeable staffing to support.

Recommendation: Ensure OT cybersecurity projects are adequately funded in Infrastructure Investment and Jobs Act (IIJA) implementation.

OMB should work with the ONCD, CISA, and SRMAs to require a minimum percentage of discretionary grant funding opportunities in the IIJA[18] and be dedicated to projects associated with OT cybersecurity or cybersecurity for IT/OT convergence. OMB should provide guidance for state, local, tribal, and territorial governments and eligible critical infrastructure owner/operators that funding provisions in the IIJA can be used for OT cybersecurity, and cybersecurity for IT/OT convergence projects.

Recommendation: Expand CISA services into OT specifically for SLTT critical infrastructure.

CISA should evaluate the creation and expansion of OT specific services offerings specifically for SLTT government owned and operated critical infrastructure.

---

[17] See 1.3, "Regulated Sectors Perspectives" for additional details.

[18] U.S. Congress, Infrastructure Investment and Jobs Act, November 2021, https://www.congress.gov/bill/117th-congress/house-bill/3684.

Many smaller critical infrastructure OT provider organizations do not have the resources to support complex cybersecurity threat mitigation and resilience capabilities. To help provide a better collective defense posture, CISA should work with SRMAs to co-develop cyber incident response and recovery playbooks as well as fund any required shared hardware, software and staff training to execute those playbooks in conjunction with DHS fly-away teams and SRMA staff.

1.3. Regulated Sectors Perspectives

Currently, the U.S. does not have a single, all-encompassing federal law that governs cybersecurity, including OT cybersecurity. However, in the absence of a general national federal cybersecurity law, the U.S. government addresses cybersecurity risks through a patchwork of federal and state laws. There are multiple statutes covering a range of cybersecurity and privacy regulations on the state level. In 2021, at least 35 states enacted bills focused on cybersecurity and about half the states provide for strengthened security measures to protect government resources.[19] In addition, there are sectoral-based regulations for individual critical infrastructure sectors such as energy, nuclear, health and finance, among others. In addition to federal and state regulations, there are mandatory cybersecurity requirements created by the private sector, such as Payment Card Industry Data Security Standards, also known as PCI DSS.

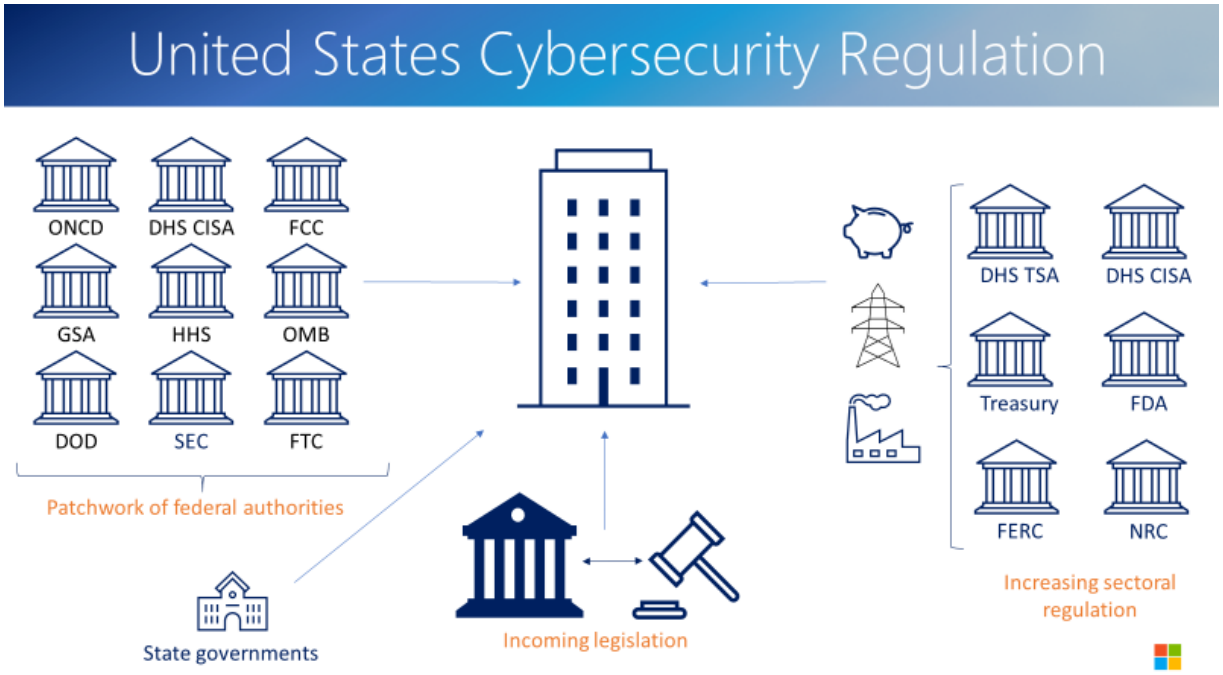

Figure 1: U.S. Cybersecurity Regulation[20]

[19] "Cybersecurity Legislation 2021," National Conference of State Legislatures, January 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.

[20] Patricia Eke, Microsoft, U.S. Cybersecurity Regulation, July 2022.

There are dozens of agencies at the federal, state, local, tribal, and territorial levels with regulatory authority over various critical infrastructure and other industry sectors, though not all regulate cybersecurity activities for their respective industry stakeholders. Regulation varies between these government agencies and in some cases may overlap. The purpose of regulation is to oversee safe, reliable, economical, and environmentally friendly services to the public. Additionally, regulated services typically receive a rate case to recover some of the costs associated with mandatory requirements.

In the context of this report, the focus will be on cybersecurity regulation of critical infrastructure that addresses safety and reliability of the services. Some of these services may include, but are not limited to, nuclear; chemical; pipeline and hazardous materials; oil and natural gas; water and wastewater; electric; transportation; and manufacturing. In some instances, these sectors are also regulated by more than one agency, including agencies from federal, state, local, tribal, and territorial governments. There may also be overlap between same-tier agencies, such as multiple agencies at the federal level. For example, the Federal Energy Regulatory Commission (FERC) and the U.S. Nuclear Regulatory Commission (NRC) regulate common infrastructure used to provide electric power. To avoid double auditing and unnecessary burdens to energy sector utilities, the two agencies signed a Memorandum of Agreement (MOA)[21] agreeing the NRC would audit infrastructure that overlaps with FERC's jurisdiction. This MOA does not relieve an entity of their compliance burden but rather allows them to interact with a single agency.

Several agencies regulate their respective sectors with mandatory cyber standards, while others may use guidelines for cyber to meet the objective of other regulations in place. Regardless of the approach for cyber, there are no specific requirements or direction on when to use IT or OT specific equipment. Rather, an objective is described, and the technology to implement is left to the company that best addresses their networked infrastructure. However, many of the requirements leave IT-focused equipment as the best solution for implementation because the OT vendor product does not fully address the requirement. For example, multi-factor authentication with a text confirmation is a capability not typically found in OT vendor equipment. As a result, to address the requirement, the company purchases an IT-centric product with supporting infrastructure for use in the OT environment.

Requiring standards is a big part of regulation. There are many approaches to determining what standard to use and how the standard is developed. As an example, the "Reliability Standards for the Bulk Electric Systems of North America"[22] standards are written for the Bulk Electric System by industry and then approved for use by FERC. The mindset behind having industry write their own standards is they should understand what is realistic in their environment but more importantly understand how the system functions. This type of approach has a slow development cycle, and it may take years to get a new requirement in place. For example, the North American Electric Reliability Corporation (NERC) has been developing a new standard for the Bulk Electric System

[21] U.S. Nuclear Regulatory Commission (NRC) and the Federal Energy Regulatory Committee (FERC), "Memorandum of Agreement Between the U.S. Nuclear Regulatory Commission and the Federal Energy Regulatory Committee (FERC), September 2015, https://www.nrc.gov/docs/ML1503/ML15033A181.pdf.

[22] North American Electric Reliability Corporation (NERC), "Reliability Standards for the Bulk Electric Systems of North America," Updated May 13, 2022, https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf.

for virtualization since 2016 and this standard is still not complete.[23] Therefore, standards need to be written objectively enough to combat cyber threats and allow for implementation of evolving technologies. With this approach, it is unrealistic to believe developing requirements will be able to keep pace with threats or technological changes, which emphasizes the importance of a well written standard that allows future adoption of technology.

Another approach is to adopt a standard that is already written. The NIST Cybersecurity Framework (CSF)[24] is an example of a framework that was written for use by multiple sectors but may not be specific enough to address risk categories for an individual sector. For example, the identification of risk for a manufacturing company may be different from the risk identified for a nuclear power plant.

The regulator should understand there is a difference between IT and OT systems and the pace of change affects the cost of doing business. For a company that is unable to increase their rates based on a rate case or if they are unable to increase rates because of customer rate tolerance, it would be helpful for the government to provide incentives/grants, low-cost loans, or subsidies to offset the additional cost of cybersecurity.

Recommendation: Ensure adequate IIJA Energy Title Funding is dedicated to OT cybersecurity projects to enable stronger security and modernization.

The IIJA Energy Title includes a rural and municipal utility cybersecurity grant and technical assistance program, for which rural electric coops and investor-owned utilities that sell less than 4 million megawatt hours/year are eligible. OMB should work with DOE to ensure that a significant portion of this grant funding is dedicated to OT and IT/OT convergence cybersecurity projects.

Regulation may require controls to address safety, environmental, and/or cybersecurity. The requirements come from jurisdictional standards and are directed by the regulator. It is not uncommon for more than one government agency to regulate the same sector. For example, the Environmental Protection Agency regulates the chemical sector for environmental safety and the Department of Transportation regulates it for transportation of the materials.[25] Because of this overlap there may be instances where requirements conflict, resulting in difficulties for the company since they must meet all requirements. Reporting events falls under this challenge as well, and it is common for a company to report operating issues to multiple agencies. For example, if a company has a cyber breach they may have to report to multiple local, state, and federal agencies, each with a different reporting form. As previously discussed, FERC and the NRC deconflicted at the government level to avoid issues with the company.

---

[23] "Project 2016-02 Modifications to Critical Infrastructure Protection Standards," NERC, accessed July 1, 2022, https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx.

[24] "Cybersecurity Framework," NIST, accessed July 1, 2022, https://www.nist.gov/cyberframework.

[25] "Chemical Sector Regulatory Authorities and Executive Orders," CISA, accessed July 1, 2022, https://www.cisa.gov/chemical-sector-regulatory-authorities-and-eos.

Recommendation: Identify opportunities to streamline OT cybersecurity regulation.

ONCD, in collaboration with CISA, should initiate an interagency study that evaluates conflicting regulations for OT operators that apply to the same sector. The end goal of this initiative would be to identify opportunities to synchronize conflicting requirements, and simplify the regulatory landscape, to better enable cybersecurity efforts by critical infrastructure entities.

1.4. Unregulated Sectors Perspectives

Some of the 16 critical infrastructure sectors have specific regulatory oversight of their cybersecurity practices. However, many owners/operators manage cybersecurity primarily through internal mechanisms with accountability to their own management and, ultimately, their shareholders and customers in the marketplace in which they compete. Sectors such as manufacturing, transportation, commercial facilities, and agriculture include a large number of private-sector participants reacting to competitive and market forces. As a result, their cybersecurity priorities are primarily motivated by operational, financial, and reputational concerns.

Many of the regulated sectors have audit results available publicly. While the company names are usually not included with the reports, information about the violations may provide insight into cybersecurity challenges. The regulator either directly or through a proxy has recurring workshops discussing how to implement the standards and cybersecurity. Many of these workshops are available to the public. Trade organizations also understand the sector and consolidate resources of their members and share that information. These trade organizations also work with the government to better understand what is expected and to represent their members. Examples of some of these trade organizations include the American Water Works Association, National Association of Regulatory Utility Commissioners, and American Petroleum Institute. Additionally, Information Sharing and Analysis Centers (ISACs) are good cybersecurity resources for their members.

A primary concern for these owners/operators is ransomware, which takes control of data and systems and holds them hostage, generally promising that the systems will be returned to service after a sum of money is paid, usually by cryptocurrency, to a difficult-to-track destination. Oftentimes, when system owner-operators pay these ransoms, they are still unable to recover their systems. This is sometimes due to the specific intent of the perpetrators, but often due to poor quality and bugs in the ransomware. Further, when an owner-operator pays a ransom and control of the systems is returned, there is no way to guarantee the integrity and confidentiality of the data and systems affected. Persistent malware threats may remain in the systems and cause recurrence of the same or similar attacks. Proper backup and recovery practices can mitigate the impact of these losses and, ideally, limit incentives to pay ransoms.

Recommendation: Promulgate lessons learned from regulated sectors.

Direct ONCD to conduct a national regulatory standard assessment every 18 months on sector-specific standards, reviewing for security gaps, alignment to a common security baseline, and duplicative standards.

CISA should work with ONCD, SRMAs and associated regulators in all regulated sectors to specifically gather lessons learned and feedback from performance metrics to determine what aspects of OT cybersecurity

regulation are specifically working well and why. This information can then be compiled by CISA, in partnership with ONCD utilizing expertise within the National Laboratories and relevant industry stakeholder organizations, to develop best practices that can be published and utilized by non-regulated entities of all types and sizes.

1.5. Public/Private Partnerships Perspectives

There are multiple industry groups that partner with CISA and the U.S. federal government on cybersecurity and critical infrastructure protection policy, strategy, and operational incident response.

On the cybersecurity policy and strategic planning front, Sector Coordinating Councils (SCCs) have partnered with the federal government on a range of joint initiatives, including updates to the National Infrastructure Protection Plan, identification of National Critical Functions and associated subfunctions, and the development of sector-specific cybersecurity plans.

Every critical infrastructure industry uses OT for production, building services, or a combination of both. However, there is no OT-specific sector coordinating council. Further, OT cybersecurity has not been a priority focus area for partnership opportunities between the SCCs and the federal government. Despite increasing cyber-attacks against OT infrastructure, CISA has not led efforts to engage multiple SCCs and Government Coordinating Councils (GCCs) on OT-specific cybersecurity public private partnerships.

In 2018, CISA partnered with the IT and communications sectors, as key foundational technology providers to multiple critical infrastructure sectors, and government officials from multiple departments and agencies to establish the Information and Communications Technology Supply Chain Risk Management (ICT-SCRM) Task Force, in order to identify and develop "consensus strategies that enhance supply chain security."[26] While the Task Force has developed multiple guidance documents and policy recommendations for government and industry stakeholders, it has not focused on deliverables on OT cybersecurity supply chain management.

CISA has organized and sponsored, under the auspices of the Critical Infrastructure Partnership Advisory Council, two entities for collaboration in the area of ICS and OT. The first is the Control Systems Interagency Working Group of which membership is from the various federal government department and agency stakeholders with ICS and OT equities. This group can be loosely thought of as a functioning GCC with regards to OT. The second group is the private sector complement to the first and is called the Control Systems Working Group (CSWG). This group has representation from stakeholders including asset owners, OEM, vendors, cybersecurity providers, standards bodies, academia, as well as other stakeholders and can be loosely considered the SCC portion of the group.

On the operational and incident response side, ISACs help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISAC staff have a strong understanding of the specific sector with which they engage. ISACs collect, analyze, and

[26] "Information and Communications Technology (ICT) Supply Chain Risk Management Task Force," CISA, accessed July 1, 2022, https://www.cisa.gov/ict-scrm-task-force.

disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.[27] There are multiple ISACs across industry sectors, as well as for state and local governments, and other entities. There is also an organization calling itself the OT-ISAC, headquartered in Singapore[28].

CISA established the Joint Cyber Defense Collaborative (JCDC) in August 2021 to unify defensive actions and drive down risk in advance of cyber incidents. JCDC Alliance Members have partnered with CISA to develop proactive cybersecurity incident response playbooks and have utilized the JCDC forum to share information and telemetry on cyber incidents as well as mitigation and response strategies and tactics. JCDC members have actively shared information relating to the Log4Shell vulnerability and are developing resources to holistically manage cybersecurity and vulnerability incidents. The JCDC is also engaging with OEMs and OT cybersecurity vendors to identify opportunities to leverage the JCDC platform to improve ICS security and incident response. At the time of this writing CISA was in the process of standing up an ICS component within the JCDC.

Recommendation: Designate a lead cross-sector OT cybersecurity partnership effort.

CISA should partner with key industry SCCs and ISACs, the ICT-SCRM Task Force, the CSWG, and the JCDC to launch a joint-sector OT cybersecurity initiative focused on strategic cross-sector, critical infrastructure protection policy and strategy, and tactical, operational response. CISA should partner with industry to identify key participants, focus areas and challenges to prioritize specific IT/OT convergence objectives for the partnership to address.

1.6. Vendor Perspectives

The challenge facing vendors and OEMs with the convergence of IT and OT technologies within critical infrastructure has largely been driven by the accelerated pace of technological innovation in the IT space coupled with the extended lifecycle of OT systems and the conservative nature of critical infrastructure operators. As OT system operators gradually began adopting IT technology, the associated IT security practices proved difficult to implement because the OT systems and devices largely didn't support typical IT security features. As a result, IT professionals began to become more involved in the security of the OT system to address the subsequent gap in the OT system security, bringing the tools that they were most familiar with, comfortable with, and trusted.

As IT professionals began applying IT security practices to OT systems, the industry began to see conflicting needs and requirements between IT and OT people, processes, and technologies. Vendors and OEMs have responded in different ways. Some have begun adding traditional IT security configuration options and technologies to their products and solutions, others have introduced technologies they felt were more

[27] "National Council of Information Sharing and Analysis Centers (ISAC)," National Council of ISACs, accessed July 1, 2022, https://www.nationalisacs.org/.

[28] "Operational Technology (OT)-ISAC," OT-ISAC, accessed August 2, 2022, https://www.otisac.org/.

appropriate given the differences between IT and OT security, and still others have attempted to enhance existing technologies.

As a result, the OT systems, and the vendors and OEMs that build products and solutions for them, are confronted with a challenge. Supporting IT security requires adding technologies and functionality to products and solutions that are built for a singular purpose. Addition of these technologies then creates an added attack surface. Further, maintenance of these technologies typically comes in the form of continuous patching cycles which requires more connectivity to efficiently deploy security critical updates, creating additional risks to the OT systems.

Given these challenges, there remains a lack of consensus on the best technologies to use to address OT system security challenges versus IT security challenges. IT security technologies generally require broader connectivity to maintain a consistent and continual patching process as well as user authentication. OT security practices generally rely on a layered defense and less connectivity to maintain physical and logical separation.

While there may be a lack of consensus, the committee finds that there is not a lack of technology to address security challenges in IT/OT converged systems. In fact, the committee has found that there is a tremendous amount of effective technology to deploy and many frameworks from which to learn and apply best practices. The prevalence of technology and different standards and frameworks may actually be contributing to inefficiencies and confusion by owners/operators. Where security technologies for IT/OT convergence are abundant, NSTAC also recognizes that developing and manufacturing devices, solutions, and software need to come under appropriate scrutiny. It is important to recognize that cybersecurity is not composed of technology or products in and of themselves. Cybersecurity encompasses everything that goes into the development, production, manufacturing, operation and management of those products and technologies.

NSTAC believes the procurement reform recommendation in Section 1.1.2 can be used to ensure that the USG only procures OT solutions that include the required technology-neutral cybersecurity capabilities. Further, the guidance developed under the recommendation can similarly drive stronger cybersecurity outcomes in private sector procurement.

1.7. People and Workforce Perspectives

The U.S. needs to incentivize the creation of enough sufficiently trained experts so that public and private sector critical infrastructure OT interests are better protected. Many of the principles of IT security, such as confidentiality, integrity, and availability, apply in OT environments. However, OT cybersecurity also requires that a high priority be placed on safety and reliability.

In addition to needing more cybersecurity professionals who understand the OT environment, we also need to understand the effectiveness of existing workforce education and training efforts to determine where gaps exist. Our initial assessment leads us to conclude that many worthwhile cybersecurity workforce training initiatives currently exist. Hands-on training is offered through the Idaho National Laboratory as part of CISA's control systems security efforts. OT specific efforts are being pursued by NIST in their National Initiative for Cybersecurity

Education initiative. Many academic institutions, including colleges and universities, are also implementing courseware and fields of study combining computer security disciplines with engineering disciplines to bridge this gap.

Yet despite these efforts, it seems clear that while the general awareness level for OT security is rising, it still is not a mainstream field of study for students to consider, and therefore it seems unlikely that a sufficient volume of experts in this area will be created through existing efforts.

The increasing number of cybersecurity threats against our critical infrastructure continues to spotlight the cybersecurity workforce gap in the United States. As a result, both IT and OT leaders in the U.S. continue to face challenges with recruiting cybersecurity talent, citing the workforce shortage as one of their top security concerns. Various workforce studies cite statistics describing the current domestic and international cybersecurity workforce shortage, but few describe the state of the IT/OT cybersecurity workforce. However, we know that there is a shortage of OT professionals today, a problem that has been years in the making due to the stigma of working in the industrial critical infrastructure profession, misaligned Science, Technology, Engineering, Mathematics (STEM) education, lack of diversity, and decline in apprenticeship programs. In addition, the aging workforce in many critical infrastructure sectors is likely to intensify the need for OT professionals across industries.

NSTAC has assessed an urgent need for IT/OT cybersecurity professionals to defend the cybersecurity posture of industrial critical infrastructure sectors as they increasingly expand their uses of technology to digitally transform their businesses. The main challenge lies in the fact that there is already a limited talent pool of IT and OT professionals. This challenge is compounded by the demand for professionals that possess both IT, OT, and cybersecurity expertise. Traditionally, IT cybersecurity professionals are educated and trained to deal with data confidentiality, integrity, and availability with systems that focus on user interaction within the environment. In contrast, OT professionals focus on physical processes' availability, safety, and reliability in systems that focus on machine-to-machine communications within the environment. As a result, these IT and OT professionals possess vastly different skills and functions and historically had little interaction. However, the advent of IT and OT converged networks requires increased collaboration between IT and OT management and teams to secure existing IT/OT networks and enable organizations to adopt new and emerging technologies.

In addition, the challenge of bolstering the number of women and underrepresented minorities in industrial STEM careers continues to be a challenge. The current critical infrastructure workforce is disproportionally white and male. For example, the workforce for the electric power generation industry is 69 percent white and 68 percent male.[29] In the manufacturing sector, 79.5 percent of the workforce is white and 71 percent is male.[30] This lack of diversity further complicates solving the IT/OT workforce shortage, intensified by the aging workforce and low public perception of working in critical infrastructure.

---

[29] "Labor Force Statistics from the Current Population Survey," U.S. Bureau of Labor Statistics, accessed July 1, 2022, https://www.bls.gov/cps/cpsaat18.htm.

[30] "Labor Force Statistics from the Current Population Survey," U.S. Bureau of Labor Statistics

While it has been changing in the last few years, there has been a tendency to require cyber professionals with a college degree, limiting the availability of applicants. This focus on college degrees has impacted immigration rules as well. The Department of Defense (DOD) is an example where they use enlisted personnel to administer many of the cyber networks. A college degree is not required for enlisted personnel. Rather, the DOD trains these cyber professionals, they receive certifications, and on the job training. A college degree is not necessary to be a competent OT cybersecurity professional.

IT leaders face challenges with recruiting IT/OT talent and retaining existing personnel. The primary concern in retaining IT personnel is ensuring job satisfaction in a demanding and resource-constrained labor market. Cybersecurity professionals are frequently overworked and tired and, as a result, more likely to experience burnout. Another obstacle in retaining cybersecurity talent is competitive hiring market conditions. As a result, mid-career professionals seeking quicker career advancement are more likely to change employers than remaining in existing positions where they might have an opportunity to build out their OT cybersecurity knowledge base.

In the federal government, retaining cybersecurity professionals is an ongoing challenge due to the slower adoption of cutting-edge technologies, limited career advancement opportunities, and a less competitive compensation structure. Retaining the government's highly qualified and experienced IT and OT talent is essential because the government is responsible for developing IT and OT cybersecurity legislation, security requirements, and best practices for critical infrastructure owners and operators. Government employees seeking quicker job advancement and professional growth working with cutting-edge technologies will likely transition to the private sector. Also, while compensation is not always a primary reason for retaining talent, it could be a factor in many cases since the government has a less competitive compensation structure than the private sector.

Recommendation: Catalog and assess efficacy of OT workforce development efforts.

The ONCD should catalog all existing OT cybersecurity workforce training and education efforts and assess the efficacy of them all and the potential of each of these efforts to scale. This should include law enforcement training efforts to help investigators gather forensic evidence of cyber-attacks in OT environments. Simultaneously, CISA should work with SRMAs to catalog programs such as the scholarship for service programs, high school programs, and internships that have a cybersecurity focus, and could be expanded to train individuals to enter the field of OT Cybersecurity. With this information in hand, ONCD, CISA and the SRMAs should then engage private sector partners to determine the market need for OT trained individuals and develop a public-private partnership to expand the service requirement in these programs to include employment at a qualified critical infrastructure company or organization.

1.8. International Partnership Perspectives

One of the challenges of multilateral cooperation on any level of IT/OT cybersecurity is the fact that there are competing interests when it comes to cyberspace, both within and between governments. Despite these

competing interests, there are shared interests when it comes to the need to secure cyberspace, notably to protect critical infrastructures and national assets, particularly in the IT/OT space.

To the extent that governments can work together to establish common best practices for securing all aspects of the technology that underpins cyberspace important to IT/OT, trustworthiness is advanced. However, in times of geopolitical conflict, governments are confronted with the imperative to use cyberspace activities that target their adversaries, such as for intelligence, disruption, and even confrontation. In those instances, this imperative undermines trustworthiness, with the risk of a loss of shared interests with business and other governments.

Yet, even in cases where governments agree on the fundamental goal of securing cyberspace, differences can occur over what constitutes effective IT/OT cybersecurity. Those differences are evident with government preferences and priorities. In some cases, individual governments face their own internal conflicts in terms of preferences and priorities, making decisions on what governments want to implement extremely difficult.

All of this points to a fundamental question posed to NSTAC by the Carnegie Endowment for International Peace: whether as buyer or regulator, are governments in a position to significantly influence what products get produced and procured, and can that influence be pursued in a cooperative and collaborative fashion with other governments?[31]

When it comes to the ability to influence, governments in market-based economies face a common set of challenges, including but not limited to:

- Governments are slow; legislative, regulatory, and procurement processes are cumbersome and do not keep pace with technological change.
- Governments can be inconsistent when it comes to developing and sustaining policy priorities.
- Expertise imbalances exist between public and private sector knowledge of technology.

Recommendation: Ensure international efforts in cybersecurity include OT.

The United States has many different vehicles for international collaboration with partners such as the newly created Bureau of Cyberspace and Digital Policy (CDP)[32] within the U.S. Department of State. The ONCD in conjunction with CISA should ensure that critical infrastructure OT cybersecurity is part of all relevant discussions. Additionally, NIST should ensure that any discussion of international standards synchronization includes OT specific standards.

---

[31] Ariel Levite, Carnegie Endowment for International Peace, "Corporate and Governmental Steps to Enhance ICT Supply Chain Integrity: Trends, Implications, and Recommendations," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 21, 2022.

[32] "Bureau of Cyberspace and Digital Policy," U.S. Department of State, accessed July 13, 2022, https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/.

1.9. Conclusion

OT systems are responsible for some of the most vital elements of our critical infrastructure, yet the security posture impact of these systems continues to be underappreciated, undervalued, and underinvested in by government and private sector alike. The convergence of OT systems with IT systems continues to accelerate, dramatically increasing the exposure of these systems to cyber threats.

The National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems represents an important step forward in securing these OT systems in key critical infrastructure sectors. As the NSM states, "the cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation."[33] The recommendations included in this report can help expand upon the initial actions included within the NSM, to ensure further progress is made in securing OT systems. They focus on concrete, actionable steps the administration can take to secure federal systems, support SLTT governments, and create incentives for critical infrastructure owners and operators.

The president should underscore the importance of addressing the risks posed by the convergence of OT and IT systems by protecting the systems that the federal government owns and operates. The successful implementation of these actions will have significant positive downstream effects to critical infrastructure security posture and will serve as a valuable model that can be replicated by SLTT governments and private-sector owners and operators of critical infrastructure to improve OT security.

[33] The White House, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

Appendix A. Technology Topics: Legacy Concerns

Over the past century, asset-intensive organizations have benefited from new emerging technologies to drive better economic, business, and societal outcomes. Programmable Logic Controllers (PLC) were introduced in the automobile industry in the late 1960s, to make efficient changes in production systems. Prior to the introduction of PLCs, making changes to or troubleshooting production systems required significant manual effort to physically inspect and adjust mechanical relays with complicated wiring. As the positive business outcomes continue to encourage the development of new capabilities leveraging emerging technologies, many factors have combined to complicate the cybersecurity challenges associated with legacy assets in operational technology (OT) environments. In this section, we lay out many of these factors and make several recommendations to mitigate the cyber risks they create.

1.1. OT and Information Technology (IT) Convergence: A Clash of Cultures

While technology advancements have enabled the fourth industrial revolution—focused heavily on connectivity, automation, and real-time data—asset-intensive enterprises have still maintained the same core risk mitigation objectives over the past century that are broader than typical cybersecurity challenges: safety of personnel and communities they serve, availability of production, and integrity of the process. Unlike their companions in IT, OT environments contain many cyber physical systems, such that what happens in the digital environment can directly impact the physical world, including the safety, production, and delivery of product. As a result of these factors, OT is grounded in a culture of safety and machine-to-machine automation where the process is highly engineered, and any change is purposeful, planned and time intensive. Comparatively, the ability for IT to impact the physical world is not as direct since IT focuses on business productivity of the user and not the direct interaction of production equipment. IT has a culture of rapid change where short cycle times of development are expected, and slow cycle times are considered negative, because they stifle efficiency. The convergence of these two environments provides the opportunity to gather data from the OT environment to support business services, such as billing for a sold product. In contrast, the OT environment typically does not have the rapid change in technology that IT has. For example, a water utility provides the same service today as it did fifty years ago; it delivers water to a customer. The process to deliver water through the piped infrastructure remains in place for decades while the purpose of the OT equipment remains the same. IT/OT Convergence, at its core, is bringing together technology capabilities with cultures clashing fundamentally over whether rapid change is good for business or is the primary driver of risk that can impact safety and availability of a product. This clash plays out in a variety of ways as described over the following sections.

1.2. Long Technology Depreciation Periods in OT Environments

As we think about IT's drive for faster innovation and efficiency, the developer's effectiveness and efficiency are central to rapid change. That means that market-leading IT organizations want to empower their employees with tools that maximize their efficiency, hence creating shorter depreciation periods of laptops, mobile devices, and servers. While many IT organizations may have three-to-five-year depreciation periods in theory, in practice users are replacing these systems in shorter periods of time to drive efficiency. Due to the non-trivial expense and

highly engineered nature of production equipment, depreciation periods of equipment in OT environments may be 20 to 30 years, if not longer. Sometimes OT assets do not have replacements, forcing operators to leave them in place, exposing known vulnerabilities to the converged IT/OT environment. While some of the automation assets are built for long depreciation periods, many of the assets they need to interact with have much shorter lifecycles before becoming obsolete, as described in the next section.

1.3. Enterprise Connectivity and Interdependence Limits Change Frequency

As OT assets evolved to drive enhancements to business outcomes, the end-to-end "system" of technology has expanded to provide various functions in the various levels of the Purdue Model, which establishes best practices for the interaction between ICS and business networks.[34]

While some assets such as PLCs are engineered for lengthy technology depreciation periods, the Human Machine Interfaces (known as HMIs) or Engineering Workstations are built to operate on platforms such as Linux or the Windows operating systems, which have much shorter depreciation periods. Therefore, it is not uncommon to encounter hardware, operating systems, or software that becomes obsolete by a vendor sooner than a field device such as a PLC. Once the vendor no longer supports a product, it is unlikely a discovered vulnerability will be addressed by the vendor. In contrast, some legacy devices may still be supported by the vendor but, because of the technical design, may be unable to meet the security requirements of today's interconnected networks. For example, these devices may not be able to accept complex passwords, provide event logging, have compatible protocols, or allow for encrypted connections such as Secure Shell Protocol, known as SSH. For legacy devices that have no replacement and are no longer supported by the vendor, the user is challenged with maintaining the functionality of the device. It is common for the user to purchase spares or replacements from a gray market supplier, which creates supply chain attack security concerns. Even when changes can be made, such as patching systems, upgrading infrastructure, or installing firmware, the interconnectivity of the OT environments requires extensive planning and risk assessments before any change can be implemented.

1.4. Historically Closed Systems Led to Assets That Were Not Secure by Design

When programmable OT assets were first developed, they commonly operated on closed loop environments, and therefore were not accessible by other traffic. Additionally, the OT environments in most cases had limited connectivity to the IT environment, usually to gather data for billing and operational statistics. As the Internet had limited commercial adoption until the early 1990s, cybersecurity concerns were not prevalent. The combination of these factors enabled ICS vendors to optimize on functionality with limited concerns regarding cybersecurity at the time. Encryption for OT protocols, which may not be necessary or desirable in many cases, is rare. Detailed event logging is also seldom employed by critical infrastructure owners and operators. The OT assets use shared, hard-coded, or well-known default credentials, and have routinely discovered vulnerabilities that are unable to be patched. This has been viewed as an accepted risk because of the lack of outside connectivity to these devices. Additionally, OT devices are relatively simple embedded devices with limited processing capability and are

[34] U.S. Department of Defense (DoD), "DoD Control Systems Security Requirements Guide Version 1 Release 1," January 26, 2021, https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/Jan_26_Control_Systems_SRG.pdf (pg. 14).

designed to meet the requirements of the environment. These OT assets typically cannot be retrofitted with cybersecurity because they lack the processing capability to perform functions other than the role designed. As a result, these legacy systems must be wrapped with more modern cyber security assets, commonly found in the IT environment.

Because of operational efficiencies and the increased need to gather data from the field control devices, these legacy systems have ethernet connectivity using internal protocol-based protocols. These legacy OT environments may have not been designed or intended to connect to IT networks but are now interconnected and discoverable by tools such as Shodan.[35] There is now broad commercial adoption of the Internet capabilities that enable the ease of cyber-attacks for criminal or geo-political gains. This connectivity, which leverages the cyber insecurity of OT assets, causes risk to the safety, availability, and integrity of engineering processes in the physical world. While the mindset, secure design practices, and risk management practices of ICS vendors and OT asset operators have improved significantly, modernization is driving connectivity of OT environments to the IT environment and cloud, creating risk for legacy assets, which may not be able to be replaced because of operational constraints.

1.5. Accidental and Unapproved Connectivity Creates Risk

Many OT environments are built in a layered model (like the Purdue model) with rings of protection that support the flow of reporting data out of the environment yet limit the ability to effect changes to assets in the environment. This architectural and infrastructure approach serves to create compensating controls against inadvertent or malicious actions against the OT equipment described in the last section. While these layers of protection naturally reduce the inherent risk of OT assets, without a highly disciplined approach to change management, understanding of the communication paths, and underlying protocols, it is common to see architectural gaps. These gaps may be a result from unauthorized or undocumented workarounds that create significant risk to the assets. This may occur for a variety of reasons, of which several real-world examples are listed here:

- An intentional communication path is put in place during urgent system troubleshooting but is never removed and is forgotten.
- A creative employee finds a way to implement a communication path to work around an overly restrictive corporate policy limiting connectivity.
- An engineer creates connectivity to accomplish a business function without awareness of the security risks being created.
- An engineer skips the IT procurement process and acquires an off-the-shelf Internet of Things (known as IoT) asset with “smart” connectivity to the cloud.

[35] “Search Engine for the Internet of Everything,” Shodan, accessed July 1, 2022, https://www.shodan.io/.

- An engineer implements a wireless access point to enable approved connectivity, yet the device is configured in ways that creates a pathway for attackers.
- A third-party automation vendor virtual private network (known as VPN) connects directly to sites that bypass security controls.
- A device is accidentally connected to the wrong port of a switch.
- Poor configuration management and documentation practices lead to misunderstanding of connectivity for the system and permissions.
- Lack of qualified staff installing, configuring, and maintaining a system leads to a "just get it working" mentality and follow-on actions that enhance exposure.
- Cyber systems that require access to the cloud, vendor, or internet connectivity for licensing verification, updates, weather feeds, etc. potentially creates undesirable connectivity to external systems and users.

Note that many of these cases are examples of why organizations go down the path of IT/OT convergence, emphasizing that the challenge is around architecture, discipline, and management - not technology.

1.6. Key Findings

1.6.1. Accept that IT/OT Convergence Will be the End State

While there are many OT engineers that may rely on the idea of an air gap to protect their environments, asset operators should recognize that in most environments the air gap is a myth. In fact, many members of the President's National Security Telecommunications Advisory Committee have 25 years-plus experience and have never seen a true "air-gapped" OT system. Organizations need to conduct business efficiently to gain a competitive advantage, and individuals will make unintentional decisions to drive access that will create cyber risk to OT assets. The business insights, cost efficiencies, and cycle time improvements to be gained through convergence are so great that organizations have already proceeded or will proceed down the path of convergence, unless precluded by doing so based on regulation. The key is understanding the risks when deciding to converge IT and OT technologies, and using cybersecurity best practices when implementing convergence.

While many organizations have an "accidental security design", our recommendation is that organizations incorporate security architecture and design as a core process to ensure they can meet the goals of efficiency and security at the same time and continue with a robust security governance and management program. While there are many options on how to accomplish this based on organizational maturity, the key is for organizations to be in a regular practice of security design and operation. Utilize resources that have the expertise to assist with the secure design and implementation, this may include using resources outside of the organization.

Inventory of the entire system is a critical first step. Understanding where the risks are and how to mitigate those systems that are unable to accept modern security controls, such as legacy devices, allows for better decision making.

Identifying a standard or guidance framework and applying it to a governance program will improve the chances of success with the recognition that not all legacy devices can simply be removed and replaced. Technology is available to accomplish the task, even if legacy devices exist. It is the discipline of the people and processes that will help achieve success.

1.6.2. Compensating Controls are an Alternative Patching and Tech Refresh

As discussed earlier in this section, in many cases vulnerabilities in OT assets can seldom or never be patched. In some cases, legacy devices may have no replacements that can be fixed with a technology refresh program. Therefore, statements like "legacy assets must be removed" is unhelpful guidance to asset operators. Certainly, the most practical advice to asset operators is to patch all vulnerabilities as frequently as possible. However, when not possible, implementing compensating controls like firewalls, network access control, segmentation, and additional monitoring around the legacy devices can provide an effective risk reduction.

1.6.3. Zero Trust Access Mitigates Security Risk

While OT operators should make efforts to upgrade obsolete assets, the pragmatic reality is that this will be a process measured in decades, while the convergence changes associated with digital transformation may be measured in months or single digit years. As such, asset owners should accept that their brownfield environments will be at risk for extensive periods. While many systems have inherent security flaws, a hybrid zero-trust architecture can be implemented that retrofits legacy systems by wrapping a layer of security abstraction around the devices that cannot be upgraded. This approach will limit the ability of personnel and unauthorized devices to connect directly with vulnerable OT assets.

Appendix B. Technology Transition/Future Thoughts

With the rollout of digital transformation initiatives in critical infrastructure and critical manufacturing organizations comes the adoption of new enabling technologies that are expected to increase productivity, improve operational visibility, reduce cost, and increase safety. At the same time, with the new technologies comes the increase in cyber-attack surfaces which could be leveraged by threat actors. The new technologies themselves can potentially introduce new vulnerabilities into critical infrastructure. In addition, the way in which those technologies are architected into operational networks can introduce exploitable vulnerabilities into critical infrastructure. This challenge can be further exacerbated if the operators' lack experience with these new technologies. In this section we examine some of the technologies that are seeing increased adoption as information technology (IT) and operational technology (OT) converge as well as some security related recommendations.

1.1. Transition to Cloud Services

IT departments are rapidly adopting cloud technologies for new workloads and migrating existing ones, and this ongoing trend will include IT/OT convergence. OT systems are intrinsically site-specific, but they increasingly report data to, and even take direction from, cloud-based or cloud-hosted software and services. These services provide commercial and operational benefits to operators but can also create new cybersecurity risks that need to be controlled. In particular, use of cloud technology can increase the risk of “accidental” IT/OT convergence, because existing security guidance for OT systems relies on network isolation to protect critical equipment from outside threats. Introducing internet-delivered services into these environments requires careful adaptation of existing controls, increasing the complexity of the network configuration, and introducing risk of accidental network exposure of assets which were meant to be isolated. Adhering to zero trust architectures (ZTA) provides effective controls for these risks, but zero trust is not yet deployed widely.

However, even advanced architectures like ZTA cannot resolve fundamental availability risks of services delivered over the internet, where disruptions of physical networking infrastructure or Denial of Service attacks can interfere with service delivery. As a result, IT/OT projects that rely on cloud services need to be designed to degrade gracefully when internet connectivity is disrupted, protecting their critical functionality. The technology and architectural practices to build systems with this property are known but are inconsistently applied, and systems integrators, cloud service providers and software developers will need to address this gap.

In addition to availability risks, data integrity and confidentiality controls change with the adoption of cloud systems. Operators want to be able to apply modern data science to their OT data to improve their operations, which often leads to the creation of "data warehouses" and "data lakes" that centralize information from many sources for easier analysis. This introduces new challenges for governing access to the data where convenience of access is both a business need and a potential risk, requiring new Identity and Access Management (known as IAM) technologies instead of relying on controlling physical access to the site. Data provenance and tracing is also important to track in case defects, whether accidental or malicious, are introduced from particular data

sources, and data dependencies need to be tracked so that downstream consumers of the data, like statistical or machine-learning models, can be updated if the source data is later found to be incorrect or compromised.

Software-as-a-Service (SaaS) architectures, which are an example of a cloud service, have cybersecurity benefits in addition to the new concerns they raise. Central administration and remote management make it easier for organizations to understand their assets, keep configurations in sync, manage software updates and ensure administrative consistency, which are often challenging for OT deployments. This also allows more efficient use of scarce workforce talent, as owner/operator organizations can centralize security incident response instead of needing to rely on having those employees at each site. In addition, Cloud Service and SaaS Providers often have their own skilled security teams and practices who can contribute to the overall security of the IT/OT solution, although the specific roles and responsibilities of the provider versus the owner/operator need to be carefully managed. SaaS is one of many cloud service options that may benefit the OT environment for all the reasons described.

1.2. Fifth Generation (5G) Cellular Networks

Cellular technology is by no means new in terms of usage in national critical infrastructure. Cellular technology has been used as a communication path for remote OT field devices and systems since its introduction. It offers a cost-effective means to transport telemetry from these remote systems to a centralized control center without building expensive infrastructure pathways such as fiber-optic or coax that require right of ways. Older cellular technologies had limited bandwidth and as a result the type of information sent was typically limited to operational and management data. As will be discussed in the following paragraphs, 5G offers the opportunity to increase that bandwidth allowing for additional data to be sent, including security data, which is typically resource demanding.

With 5G, the improvements are expected to be dramatic with 100X increase in bandwidth, 10X reduction in latency and 100X increase in network capacity, relative to its Fourth Generation (4G)/Long-Term Evolution (LTE) predecessor. This exponential increase in capabilities is expected to enable a new set of applications from massive Internet of Things (IoT) sensors, virtual reality/augmented reality, connected transport, smart cities, smart factories, smart hospital private networks, remote operations via robotics (maintenance, surgery) and more.

Many of these applications will be characterized by patching for IoT devices, data driven operation, data and device containment, monitoring, secure data flow, vendor and partner involvement, encryption, and integrity protection for signaling and user data.

Commercial cellular networks introduced using special purpose hardware, the introduction of iPhone and smartphone apps, and software-defined networking (known as SDN). The latest additions to 5G networks have been LTE, the 5G Standalone core, Hyperscaler, and Open Radio Access Networks (or RAN).

As with any other new technology, 5G will come with a new set of vulnerabilities that will need to be managed properly to reduce the risk of attackers leveraging the associated attack vectors to compromise critical infrastructure (CI) organizations. Some of the threat vectors associated with 5G[36] include:

- **5G Systems Architecture** - The sheer magnitude of connected 5G devices will increase the overall vulnerability footprint for both legacy and new devices. Furthermore, 5G also leverages other technologies (e.g., software defined network, cloud native infrastructure, network slicing, edge computing) and legacy networks (e.g., 4G LTE) which introduce other attack vectors per se. Since 5G technology will be increasingly leveraging predominantly IT infrastructure, the risk of IT being compromised and being used to pivot into OT heightens. Organizations who use 5G for wide area network connectivity (backhaul) will typically be dependent on 5G service providers for connectivity. Subsequently, this results in loss of visibility in terms of any cyber risk associated with using 3rd party infrastructure. Similarly, even when using 5G private network technology, there could be loss of visibility to network traffic and any underlying threats due to the 5G protocol encapsulation which masks the network traffic. ZTA implementation is expected to play an important role in protecting 5G Networks. ZTA in 5G networks will be characterized by firewall and perimeter protection of the 5G core, encrypted traffic, identity life cycle practices, least privilege access policies, continuous scanning of software, security event logging, and micro segmentation around each core.

- **Supply Chain** - The 5G supply chain will be susceptible to risks associated with 5G devices/systems that have software/hardware "backdoors" or other malicious code or components which are easy to compromise because of poor design and/or maintenance support. The supply chain will also be subject to trade restrictions enacted to protect national security.

- **Policy and Standards** - This vector is tied to the risk associated with an organization's or nation state's intentional shaping of 5G standards to benefit their proprietary technologies and limit end users' choices to use alternate offerings. There may also be cases where optional security controls have been defined yet these controls if not implemented could lead to substantial security gaps.

While the full 5G architecture and technology ecosystem is expected to evolve and expand, there are several recommendations organizations can still consider facilitating better awareness and adoption of 5G cybersecurity practices. These are provided in the recommendations section below along with other general recommendations about advanced technology adoption.

1.3. Next-Generation Communication Technologies

In addition to 5G cellular communications, there are other emerging and next-generation communication technologies that designers, architects, operators, and cyber risk professionals must be aware of. These next

[36] CISA, National Security Agency, and Office of the Director of National Intelligence, "Potential Threat Vectors to Fifth Generation (5G) Infrastructure," 2021, https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf.

generation technologies must ensure future proof architecture based on Third Generation Partnership Program (3GPP) standardized networks that can be upgraded to the next technology with minimum disruption and provide backward compatibility of devices and applications.

One example is LoRa (derived from 'long range') which is a radio frequency modulation technique using license-free spectrum in sub-gigahertz frequency bands (902–928 megahertz (MHz) in North America) to provide a low-power, low-bit rate, long-range communication system (LoRaWAN) for IoT networks. With typical ranges of up to 15 kilometers and bit rates of up to 50 kilobytes per second (kbits/s) per channel, LoRa is ideal for low-power IoT sensors such as smart meters, leak detectors, soil moisture sensors, and smart street lighting controllers dispersed over a relatively large area. Another example is the Starlink satellite constellation currently being deployed by SpaceX to provide high-speed Internet access. The Starlink service is provided via a small dish and router device provided by SpaceX, is mobile, and delivers advertised speeds up to 150 megabits per second (Mbp/s) for residential consumers and a higher-speed option of up to 500 Mbp/s for business and enterprise use.

Both examples, as well as others emerging technologies, introduce new capabilities for delivering IT and OT network communications but also introduce potential risks to those environments. These technologies are primarily radio frequency based and therefore wireless. As with any wireless technology, certain vulnerabilities are present such as signal jamming and signal interception, especially in the absence of effective payload encryption. With the wide availability of inexpensive software defined radios, signals, and systems typically out of reach and view of attackers are now easily viewed and potentially accessed and modified. Many of these technologies also rely on new and occasionally proprietary network protocols that have not been "battle tested" with wide deployments and security review. Finally, with the costs of many of these technologies well within reach of even individual users, operators of critical infrastructure must be aware of the potential for shadow or rogue networks connected to their operation networks.

While next-generation communication technologies provide exciting and innovative capabilities for designers and operators of critical networks, awareness of accompanying potential cyber risks must also be factored into the governance and protection of these networks. Critical network operators must continuously pay attention to these emerging capabilities and threats.

1.4. Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning (AI/ML) are also starting to gain adoption in national critical infrastructure OT. These include for example systems for predictive maintenance and production optimization using data from a variety of data inputs such as IoT sensors to perform analytics and provide insights. AI/ML applications even include cybersecurity use cases for automated detection and response. In some cases, the recommendations from AI/ML may be automated to increase efficiency and shorten response time. Increasingly AI/ML systems are cloud-based and even provided as SaaS offerings by ICS/Supervisory Control and Data Acquisition (SCADA) system vendors.

While AI/ML adoption in OT environments has yet to hit critical mass, it is not hard to see how such systems could be more widely deployed in the near future. That said, attackers will be more incented to target AI/ML systems, and this elevates the risk associated with these systems:

- **Attacks which take AI/ML systems offline** - Attackers could for example install malware onto AI/ML systems or the connectivity from these systems to the downstream systems which depend on their outputs. Such attacks could lead to substantial loss of productivity and possible impact to health and safety.

- **Attacks which take control of AI/ML systems** - In this scenario, attackers take control of the system or the inputs to a system such that they produce outputs which could lead to decisions on downstream systems which in turn lead to disastrous outcomes. The riskier scenario is where attackers can control the automated responses to the recommendations.

Appendix C. Cyber Insurance Implications in Cyber Physical Systems

Insurance is a critical risk mitigant to the operability and resiliency of businesses within the critical infrastructure sectors which rely heavily on operational technology (OT). These businesses range from chemical producers to water treatment facilities to the defense industrial base, and they are essential to the functioning of our society. Insurability is critical to the existence of these companies and yet there are some alarming gaps that deserve our attention. First, it can be difficult for OT owners and operators to find or afford insurance policies covering non-physical business interruption, meaning, they are unable to conduct business because of an event such as a blackout, infrastructure failure or cyber-attack. The ransomware attack on Colonial Pipeline was an example of such an attack. Second, it can be difficult for OT owners and operators to find and afford insurance covering physical damage and harm to people or property resulting from a cyber-attack, which could be considerable or even catastrophic in its impact. Fortunately, we have not seen an example of such an attack yet in this country. In both cases, OT owners and operators may be unaware of the exclusion of these events from coverage under their policies, which creates unmanageable risk for them and the critical sectors writ large.

In the 1990's when businesses began to experience cyber-attacks, cyber insurance covers were added to existing liability policies. Later, in the 2010's, in response to the growing cybersecurity risk faced by businesses, cyber liability insurance began to be sold as a standalone product. Cyber insurance products have evolved even further in the 2020's because of skyrocketing losses owing to cyber-attacks. Especially for companies within the critical sectors, a lack of understanding of cybersecurity risk has led underwriters to set policy prices extremely high and this continues to be the case. Cyber insurance products for critical infrastructure are difficult to price mainly because there is a lack of data about cyber incidents at critical infrastructure companies that have resulted in physical damage or injury available to insurers because there simply haven't been very many such incidents thus far. More data on more incidents is needed for risk to be properly assessed so insurance products can be appropriately and sustainably priced.

The difficulties underwriters face in measuring risk for OT-heavy companies introduces uncertainty about the insurability of such companies and, by extension, of certain critical sectors. Underwriters' expertise in assessing the risk associated with OT is weaker than their expertise in assessing risk associated with information technology (IT). They often lack understanding of cyber risk in these types of companies, in part because of lack of monitoring tools. Understanding attackers' tactics, techniques, and procedures (not to mention motives) for compromising OT systems is very different from IT systems. Underwriters perform annual assessments, but these annual assessments only give a static snapshot of the exposure. Companies continuously evolve their systems when they onboard new technology or acquire new assets, and cyber threat actors are constantly looking for new vulnerabilities and exploits. Underwriters' assessments of risk can therefore vary from year to year, creating instability in premiums.

For their part, owners and operators of critical infrastructure companies are far more afraid of negative assessments which could make them uninsurable than they are even of exorbitant costs. That said, they do not have a dependable way of knowing what underwriters will ask for. Increasingly, insurers are excluding cyber-

attacks from general liability or property policies via a "cyber-attack exclusion clause," or "CL 380," leaving companies in limbo as to how to protect themselves from this kind of risk. In short, owners and operators' management and boards face serious challenges in insuring themselves for cyber-attacks.

On the positive side, insurance requirements are driving change in such companies' adoption of cybersecurity best practices. Owners and operators know that underwriters expect them to have adopted minimum cybersecurity controls, including end to end encryption, multi-factor authentication, anti-phishing, privileged account management, etc.

The U.S. government may be able to do several things that can ensure owners and operators have access to affordable insurance coverage. The Government Accountability Office recently released a report that recommends a study on whether more federal assistance is needed to ensure availability of cybersecurity insurance for critical infrastructure owners and operators. The report recommended that the Cybersecurity and Infrastructure Security Agency and the Federal Insurance Office, under the U.S. Department of Treasury, should jointly assess whether risks to critical infrastructure industries warrant a potential federal response, and to report to Congress on the results of this assessment.[37]

In addition to this study, the government should encourage the creation of – or create itself – a body of data around cyber incidents affecting critical infrastructure. The President's National Security Telecommunications Advisory Committee supports and reiterates the Cyberspace Solarium Commission report's[38] recommendation that Congress create a bureau that would collect and publish information on cyber incidents which could help inform insurance price setting. Second, the government could ask insurers to standardize language contained in insurance policies, so that it is clear to owners and operators where coverage of physical damage and liability owing to a cyber-attack resides, or if it is excluded. Third, the government can assist by ensuring there is awareness amongst owners and operators that there may be gaps in their coverage for cyber-attacks. Awareness of gaps in cyber insurance policies should help drive demand for comprehensive coverage, which will in turn create more data and allow insurers to price more accurately for the risk. Finally, the government must articulate the conditions of a cyber-attack against critical infrastructure that has such catastrophic impacts on property and health that the government would necessarily become the insurer of last resort and must plan for this eventuality, even if we hope to avoid it.

[37] U.S. Government Accountability Office, "CYBER INSURANCE: Action Needed to Assess Potential Federal Response to Catastrophic Attacks," June 2022, https://www.gao.gov/assets/gao-22-104256.pdf.

[38] U.S. Cyberspace Solarium Commission, "Report," March 2020, https://www.solarium.gov/report, p. 78.

Appendix D. Existing Best Practices for Converged Operational Technology (OT) Networks

1.1. Introduction

This section will focus on some of the differences that the committee recommends integrators and system owners consider when designing, maintaining, and upgrading their OT systems.

There are many frameworks to select from when considering best practices for OT and information technology (IT)/OT converged systems[39][40][41]. Internationally recognized standards and frameworks all generally provide similar guidance, so the committee does not necessarily recommend one framework or standard over another. That said, the committee does recognize an inherent risk in adopting standards or frameworks that are overly prescriptive in the technologies required for compliance to the standard. Considering this, the committee does recommend choosing a particular standard or framework that suits the needs of the organization, learning it fully, and applying it rigorously.

In general, applying best practices begins with understanding the goals, personnel, assets, components, workflows, traffic flows, and dependencies of the system of interest. A second step is to identify and plan security controls. The selected security controls need to support the business and system goals, adhere to stated security policy, and operate within the system requirements. A governance program should be established to monitor and manage the implementation of these best practices[42].

The third step in applying best practices is to research, validate, and approve technologies that support the requirements of the system. There are many good existing technologies that can assist with security in industrial control systems (ICS); however, keep in mind that ICS have unique considerations that make it different from traditional IT systems. The security placed on a system should always align with the system's operational goals[43].

With this in mind, the fourth step is to determine zones of trust in which security controls can be applied in an appropriate and maintainable manner. The goal here is to minimize the zones of trust to contain only components that absolutely need to trust each other[44]. The selected controls and technologies, along with the existing system architecture, dictate how granularly we can define the zones of trust. Finally, test for operational and security needs, and continually evaluate and learn to improve both our operational and security stances.

---

[39] "Cybersecurity Framework," NIST, accessed July 1, 2022, https://www.nist.gov/cyberframework.

[40] "CIS Controls," CIS, accessed July 7, 2022, https://www.cisecurity.org/controls/.

[41] "ISA/IEC 62443 Series of Standards - ISA," isa.org, accessed July 7, 2022, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[42] NIST, "Cybersecurity Framework."

[43] CIS, "CIS Controls."

[44] CIS, "CIS Controls."

1.2. Zero Trust in ICS

Zero trust and zero trust architectures are becoming the de facto standard for IT network security and are starting to be considered and adopted on a limited basis within the OT side of industry. The goal of zero trust is to identify and remove instances of implicit trust within the system architecture, but this does not mean that we can eliminate trust from the system altogether[45]. NIST SP 800-207 specifically addresses the need for constant re-evaluation of trust within a zero-trust architecture. Therefore, we recommend that system operators and owners be aware of where they are placing trust within a system, why they are trusting the particular technology, device, control, person, etc., and when that trust is no longer valid.

As the President's National Security Telecommunications Advisory Committee (NSTAC) learned from industry briefers, the main differences in zero trust for IT systems versus zero trust for OT systems becomes evident when considering the use cases of each. IT systems generally have a strong focus on accessibility and confidentiality of the system, where OT systems prioritize availability and determinism. These separate requirements drive the need for differing and sometimes competing security technologies. Where encryption of data might be of paramount importance in IT systems, in many cases it does not provide much of an added benefit in OT systems. Conversely, where availability might be critical in an OT safety or protection related system, IT systems may be able to tolerate lower availability numbers, such as a delay in receiving an email or slower speeds for website downloads.

NSTAC recommends public and private sector OT stakeholders review the *NSTAC Report to the President on Zero Trust and Trusted Identity Management*[46] to identify potential opportunities to apply zero trust best practices in OT environments. In particular, the Committee recommends that the Cybersecurity and Infrastructure Security Agency and appropriate Sector Risk Management Agencies establish an interagency working group to create OT-specific Zero Trust Maturity Models where applicable for how to protect relevant OT services (see 1.1.6).

[45] Scott Rose et al., NIST, "Zero Trust Architecture," August 11, 2020, https://doi.org/10.6028/NIST.SP.800-207.

[46] President's NSTAC, "NSTAC Report to the President on Zero Trust and Trusted Identity Management," February 2022, https://www.cisa.gov/nstac-publications.

Appendix E. An Approach to Supply Chain Security

The committee recognizes that there exist several resources that organizations can use to learn and apply robust and best practice supply chain security techniques[47][48][49]. Resources like National Institute of Standards and Technology Special Publication 800-161 can be used to identify best practices and resources like the Edison Electric Institute's *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk* can be used to help organizations specify vendor requirements as part of the procurement process. These are thorough and well-developed resources.

Instead of reproducing the content of these resources, the committee will emphasize a few general observations about how organizations can approach supply chain security. In short, organizations benefit from a collaborative approach to working with their suppliers and vendors to address supply chain risks. True partnerships focus less on box checking exercises and more on relationship building. These relationships are critical because the complexity of the global supply chain is beyond what any single organization can reasonably control, therefore trust in suppliers and vendors is necessary to reduce the complexity for the organization. This trust is best built through collaborative relationships.

1.1. Trusted Supply Networks

Evaluation and selection of vendors to provide necessary business products and services is a continual process. This is best performed as a collaborative effort between the business function, quality, and purchasing. As this team works with vendors, it is important that the process be an ongoing effort where team members with various areas of expertise participate in the component selection, vendor monitoring, and onsite audits.

It is important to build relationships with suppliers. Onsite audits can be used to verify that vendor quality and security processes meet requirements. This knowledge should not stop at first-tier suppliers. It is important to ask these first-tier suppliers about their supply chain security practices and understand who their first-tier suppliers are. Additionally, trusted suppliers should have a supply chain risk and mitigation process to which they can demonstrate adherence.

1.2. Product Integrity and Availability

It is important for an end user to ensure that the products they receive are what they expected to receive. To do this, it is important for end users to buy directly from the manufacturer, or through the manufacturers' official distribution channels. Once the products or services are received, it is recommended that their performance be

---

[47] Edison Electric Institute, "Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk Version 2.0," May 2020, https://www.eei.org/-/media/project/eei/documents/issues-and-policy/eei-law---model-procurement-contract-language.pdf.

[48] Jon Boyens et al., "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," NIST, May 5, 2022, https://doi.org/10.6028/NIST.SP.800-161r1.

[49] NERC, "CIP-013-1: Cyber Security - Supply Chain Risk Management," accessed July 7, 2022, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf.

verified against specification. This verification is especially important if products are procured using non-official distribution channels.

If products are procured from non-official distribution channels, end-users should consider means by which to verify product performance and counterfeit detection. This may include rigorously testing the applicable functions of the product, comparison of the product to known officially sourced products, and reaching out to the manufacturer to understand the expectations and limitations that independently sourced products carry.

It is important to work with suppliers and vendors to ensure that all parties keep a sufficient supply of critical parts and supplies, as deemed reasonable. Supply chains that work to limit the distance traveled of critical parts and components are preferable given the sudden and global impact that supply chain shock can have. Materials, components, and products sourced within the United States limits some impact of global supply chain challenges.

1.3. Quality and Cybersecurity

Quality and cybersecurity are intractably linked. Organizations are encouraged to develop and maintain information security, quality, safety, and environmental management systems and ensure that their vendors and suppliers do as well. Many internationally recognized standards exist to help organizations maintain appropriate processes.

It is not uncommon for threat actors to target smaller companies with less sophisticated quality and security controls as a means to infiltrate larger end users. As such, organizations should collaborate with their vendors to understand the full quality and security capabilities of their suppliers to assess and mitigate risk as necessary.

When a vendor identifies a security vulnerability in a product or solution, the vendor should have appropriate means to alert customers and end users of the vulnerability, the risk, and mitigations or compensating controls. Vendors should be capable of quickly providing patches or compensating controls. If customers cannot be informed privately and individually, the use of well-established and well-known tools and services should be used, such as the National Vulnerability Database.

Appendix F. Limiting Cyber/Physical Impacts to Breached Systems

1.1. Resiliency (Continued Operation While Breached)

Information technology (IT)/operational technology (OT) convergence brings both benefits and risks to the resilience (or resiliency) domain of operational systems. Meanwhile, the definition of resilience continues to evolve and blend with additional domains, such as reliability and recovery, until the term becomes a buzzword or an unreachable goal. We propose a more concise definition of resilience, examine the benefits, and risks that IT/OT convergence bring to resilience, survey the existing resilience frameworks and models, and recommend a few areas of improvement.

1.2. Defining Resilience

Defining resilience is not trivial. The National Institute of Standards and Technology (NIST) lists ten variations for the term resilience in their glossary.[50] Some definitions are specific to cyber resilience, which does not fully incorporate the capabilities of operational systems. Grid resilience can be used as an example to develop a more rigorous definition of resilience for our purposes of examining IT/OT convergence. JD Taft, PhD., examines several definitions of grid resilience in *Electric Grid Resilience and Reliability for Grid Architecture*.[51] He notes that attempts to define and quantify a concept of resilience for electric power grids have mostly relied upon ad hoc definitions that are often closely tied to reliability. Many definitions include recovery. The National Infrastructure Advisory Council 2009 definition "the ability to reduce the magnitude and/or duration of disruptive events" [52] is too general to be practical and is combined with reliability.

Presidential Policy Directive 21 defines resilience for the grid as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[53] Similarly, the Department of Energy's (DOE) definition is "[t]he ability to prepare for and adapt to changing conditions and recover rapidly from operational disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[54] Both definitions fuse resilience and reliability by including recovery. This results in resilience metrics that are reliability measures. Expectations for resilience become excessive when the system must not only withstand disruptive events and minimize damage

---

[50] "Glossary: Resilience," Computer Security Resource Center, accessed July 5, 2022, https://csrc.nist.gov/glossary/term/resilience.

[51] JD Taft, Pacific Northwest National Laboratory (PNNL), "Electric Grid Resilience and Reliability for Grid Architecture," November 2017, https://gridarchitecture.pnnl.gov/media/advanced/Electric_Grid_Resilience_and_Reliability.pdf.

[52] National Infrastructure Advisory Council, "Critical Infrastructure Resilience Final Report and Recommendations," September 2009, https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

[53] The White House, Presidential Policy Directive -- Critical Infrastructure Security and Resilience, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[54] "Resilience," U.S. DOE Directives Program Office of Management (MA-1.2), accessed July 5, 2022, https://www.directives.doe.gov/terms_definitions/resilience.

but also recover from the events. The term resilience borders on becoming an all-encompassing buzzword, not a clear, practical definition with metrics that organizations can use to show management and improvement and to determine return on investment.

Building on Taft's definition of grid resilience, a perfectly resilient industrial or operational system would not experience outages and so any definition or metric that is based on measuring outage times, extents, or impacts on customers or systems would not apply. Resilience applies to the operational system under stress. Resilience can be described as resisting losing capabilities despite the stress (stress resistance) or degrading gracefully (strain adjustment), both without disrupting operations. As Taft notes, reliability measures are not useful for quantifying resilience because resilience is in large part about what does not happen.

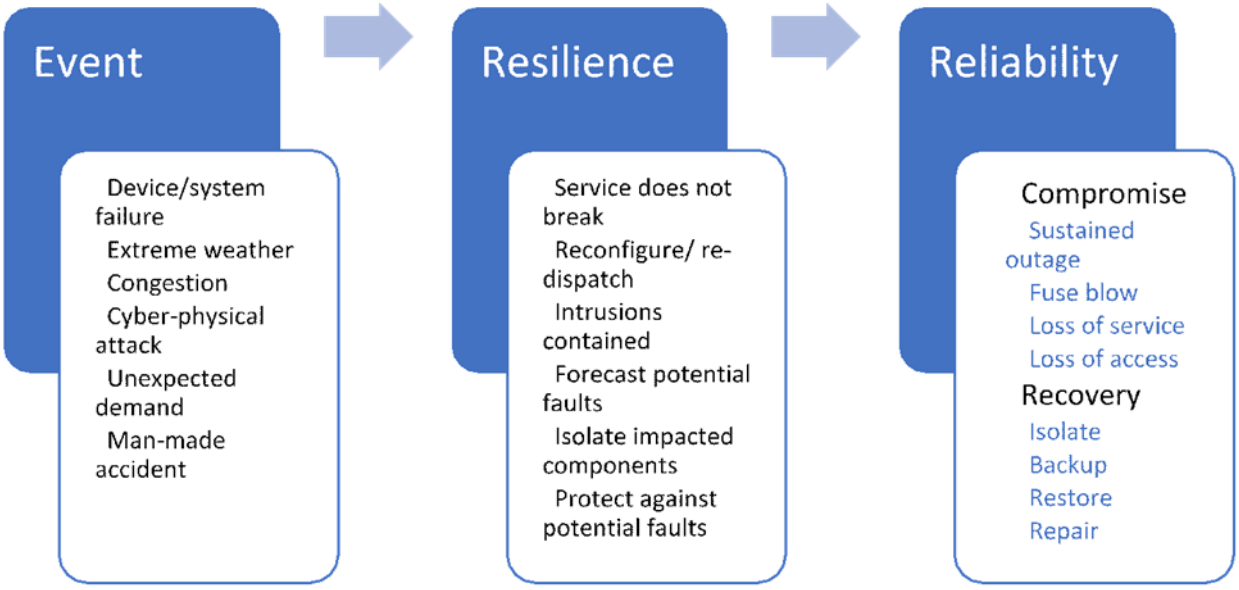

Figure 2: Characterization of Resilience and Reliability Domains[55]

For our purposes, resilience can be defined as the ability to withstand stress events without suffering operational compromise or the ability to adapt to the strain to minimize compromise via graceful degradation. It is about what does *not* happen to operations or consumers of the operational services. The resilience domain includes resistance to stress caused by the event, deformation, and compensation for the strain of the deformation on the operational system. As shown in Figure 2, the start of a sustained outage is the transition from the resilience domain to the reliability domain. Defining resilience allows us to scope the discussion on the benefits and risks of IT/OT convergence on resilience.

[55] JD Taft, PNNL, Electric Grid Resilience and Reliability for Grid Architecture, November 2017, https://gridarchitecture.pnnl.gov/media/advanced/Electric_Grid_Resilience_and_Reliability.pdf.

1.3. How IT/OT Convergence Improves Resilience

An organization can use elements of IT/OT convergence to improve the resilience of operational systems by protecting them prior to an event, then compensating for the stress and strain of the event. Prior to an event, the organization can take steps to monitor asset health and put preventative maintenance programs in place. Amazon Web Services notes that operators need to know when a machine is about to fail so they can better plan for maintenance.[56]. For example, a manufacturer might have a machine that is sensitive to various temperature, velocity, or pressure changes. When these changes occur, they might indicate a failure. Machine learning models based on data for each component of the system can evaluate data from the manufacturing system in near real-time. The manufacturer can utilize the data to repair before failure. IT/OT convergence further improves resilience by improving network performance to transmit the maintenance data in real-time.[57]

Another way that IT/OT convergence can improve the resilience of operational systems prior to an event is through hardening installations and systems hardening. Examples of hardening installations for electricity systems include momentary ride-through by highly coordinated relay protection schemes, equipment sized to handle excursions, and using reclosers to clear momentary upsets.[58] Examples of hardening systems include many cyber hygiene practices such as reducing external exposure, patching Internet-accessible systems, segmenting networks to protect programmable logic controllers (PLCs) and workstations from direct exposure to the internet, validating legitimate business needs for internet access, active monitoring, and rapidly responding to intrusions and disabling unnecessary services.[59] IT/OT convergence can enable effective protection from security threats and the optimization of the use of equipment and staff in response to events.

IT/OT convergence can enable capabilities for compensating for stress and strain on the operational systems through intelligent or "smart" equipment and monitoring. Many organizations have enhanced their monitoring, communications, and IT infrastructure to improve operational efficiencies and the resilience of their operational systems. Intelligent equipment, such as smart switches, smart metering, sensors, smart regulators and coordinated relay protection schemes aid in the acquisition, transmission, and storage of data, which is then analyzed for improved decision-making. Real-time and near real-time monitoring provide the data for organizations to know what is happening and when, then react more quickly to changing conditions. With faster and Artificial Intelligence-enhanced analysis of data from these complex systems, from anywhere in the world, decision-making could be fast enough to minimize the stress on the operational system. More complete monitoring and access to real-time converged data improves decision-making by providing a more complete

---

[56] Kevin Oleniczak, "Using Amazon Web Services (AWS) IoT for Predictive Maintenance," Amazon Web Services (blog), June 28, 2022, https://aws.amazon.com/blogs/iot/using-aws-iot-for-predictive-maintenance.

[57] Sophie Borgne, "IT/OT Convergence in the New World of Digital Industries," Schneider Electric (blog), April 13, 2021, https://blog.se.com/sustainability/2021/04/13/it-ot-convergence-in-the-new-world-of-digital-industries.

[58] Mesa Associates, "Designing your Substations for Grid Resiliency," accessed July 1, 2022, https://www.exacterinc.com/resources/uploaded/Brochures/Substation Resiliency - Jeff Keller Mesa Eng.pdf.

[59] "Alert (AA20-205A) National Security Agency (NSA) and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems," CISA, Revised October 24, 2020, https://www.cisa.gov/uscert/ncas/alerts/aa20-205a.

operating picture to the organization, leaders, and employees. Improved networking enables access to real-time information.

IT/OT convergence can also enable compensating for stress and strain on the operational systems through operational means such as adding renewable energy sources and reducing demand. For example, for telecommunications facilities, diesel generators traditionally provide backup power. Adding renewable energy sources, such as photovoltaics, can double the amount of time a site can survive an outage and continue operations.[60] To aid in reducing demand, sensors can perceive peak load problems and automatically switch to divert or reduce power in strategic places, removing the chance of overload and the resulting power failure. Advanced metering infrastructure offers time-based rate programs to consumers. Smart customer systems such as in-home displays can make it easier for consumers to change their behavior and reduce peak period consumption based on information on their power consumption and costs. These programs can help with resilience while also helping electricity providers save money through reductions in peak demand and the ability to defer construction of new power plants and power delivery systems.[61]

Aligning IT and OT systems may also eliminate unneeded hardware and software or reduce development efforts to reduce capital and operational expenses. Integrating OT systems with cloud services also benefits resilience through often improved cyber security capabilities and scalability. Cloud services can enable traceability and monitoring of cloud and on-premises resources through a centralized operations hub. The advantages of centralizing asset tracking go well beyond simplified asset loss prevention and extend to maintaining compliance of patches and configurations and responding to incidents.[62]

1.4. Risks to Resilience

IT/OT convergence benefits resilience while also bringing risks to resilience. IT and OT systems are distinct systems with their own priorities. Organizations often have separate teams to architect, maintain and protect IT systems, and architect, maintain and protect OT systems. When evaluating resilience, the interconnectedness of these two technologies and their criticality to the organization should be evaluated as a system of systems, not separately. The Colonial Pipeline ransomware incident, the Triton attack and the NotPetya attack are examples of how the integration of IT and OT systems can impact resilience whether the attacker targets the IT systems and unintentionally impacts the OT systems, or uses the IT systems to reach the OT systems.

The Colonial Pipeline incident is an example of the attackers targeting the IT systems and unintentionally impacting the OT systems. On May 7, 2021, Colonial Pipeline announced that they were the victim of a ransomware attack and halted product delivery as a precaution. Colonial Pipeline provides almost half of the fuel

---

[60] Society of Cable Telecommunications Engineers and International Society of Broadband Engineers, *Journal of Energy Management Volume 2 Number 2*, August 2017, https://www.nrel.gov/docs/fy17osti/69034.pdf.

[61] "Demand Response," U.S. DOE Office of Electricity, accessed July 18, 2022, https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/demand-response.

[62] AWS, "Security Best Practices for Manufacturing OT," May 2021, https://d1.awsstatic.com/whitepapers/security-bp-for-manufacturing-ot.pdf.

supply for the East Coast.[63] Organizations may assume that IT system compromises would not impact OT systems, and the OT systems could continue to operate manually without depending on IT systems, common software applications and data sets. Pipeline systems, like other OT systems, have increasingly interconnected control systems and business systems to enable demand forecasting, locational marginal pricing, and hourly transaction clearing to increase the cost efficiency of delivery over large operating territories. Accomplishing all of this requires near-real-time access to OT system sensor data to accurately account for billing transactions.[64] Dragos has found that organizations think that their IT networks are segmented from their OT networks. The reality is that segmentation has atrophied over time through misconfigurations, additional devices, or business needs.[65]

The TRITON malware (named HatMan by the Department of Homeland Security (DHS)) follows Stuxnet and Industroyer/CrashOverride in specifically targeting devices found in OT environments, but can directly interact with, remotely control, and compromise a safety system.[66] The attackers moved from the IT network to the OT network through systems that were accessible to both environments. Traditional malware backdoors, Mimikatz distillates, remote desktop sessions, and other well-documented, easily detected attack methods were used throughout these intrusions.[67] The targeted systems provided emergency shutdown capability for industrial processes. Mandiant assessed that the attacker was developing the capability to cause physical damage and inadvertently shutdown operations.[68]

NotPetya did not target industrial environments specifically. But due to its self-spreading capabilities and its use of an SMB vulnerability present in many OT environments, it impacted many industrial sites and required hundreds in millions of dollars to recover for some.[69] On June 27, 2017, NotPetya impacted banks, airports and power companies in Ukraine, Russia and parts of Europe.[70] The Department of Homeland Security (DHS) reported that the malware campaign infected the finance, transportation, energy, commercial facilities, and

---

[63] FERC, Statement from FERC Chairman Richard Glick: Chairman Glick and Commissioner Clements Call for Examination of Mandatory Pipeline Cyber Standards in Wake of Colonial Pipeline Ransomware Incident, May 10, 2021, https://www.ferc.gov/news-events/news/statement-ferc-chairman-richard-glick-chairman-glick-and-commissioner-clements.

[64] Jonathan Monken and Maggie Smith, Modern War Institute at West Point, "The Colonial Pipeline Hack Shows We Need a Better Federal Cybersecurity Ecosystem," June 1, 2021, https://mwi.usma.edu/the-colonial-pipeline-hack-shows-we-need-a-better-federal-cybersecurity-ecosystem/.

[65] Mike Hoffman and Tom Winston, "Recommendations Following the Colonial Pipeline Cyber Attack," Dragos, May 11, 2021, https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/.

[66] CISA, "Malware Analysis Report-17-352-01 HatMan—Safety System Targeted Malware (Update B)," February 27, 2019, https://www.cisa.gov/uscert/sites/default/files/documents/MAR-17-352-01 HatMan - Safety System Targeted Malware %28Update B%29.pdf.

[67] Steve Miller and Evan Reese, Mandiant, "A Totally Tubular Treatise on TRITON and TriStation," June 7, 2018, https://www.mandiant.com/resources/totally-tubular-treatise-triton-and-tristation.

[68] Nathan Brubaker et al., Mandiant, "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure," December 14, 2017, https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton.

[69] Amir Preminger, Claroty, "NotPetya: Looking Back Three Years Later," June 30, 2020, https://claroty.com/2020/06/30/notpetya-looking-back-three-years-later/.

[70] David Bisson, Tripwire, "NotPetya: Timeline of a Ransomworm," June 28, 2017, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/.

healthcare sectors.[71] The delivery mechanism of NotPetya during the June 27, 2017, event was determined to be the Ukrainian tax accounting software, M.E.Doc. The cyber threat actors used a backdoor to compromise M.E. Doc's development environment as far back as April 14, 2017.

The Colonial Pipeline ransomware incident, the Triton attack, and the NotPetya attack are a few examples of how the integration of IT and OT systems can be exploited by intentionally or unintentionally traversing IT and OT networks, and either bringing down or severely degrading operations. As IT and OT converge further, their vulnerabilities and risks become more closely tied together. Their combined impact on the resilience of the organization will become more complicated and potentially much greater.

1.5. Survey of Resilience Frameworks and Models

Several resilience frameworks and models exist to help organizations understand risk and improve the ability of their systems to continue operating despite the stress and strain of an event. The sampling of incidents in the previous section shows the importance of evaluating IT systems and OT systems together when applying a resilience framework or model. Because of the state of IT/OT convergence, the people that acquire, operate, and maintain the IT systems and the people that do the same for OT systems, their processes, and their systems should be assessed together.

Cyber Resiliency Engineering Framework[72]: NIST Special Publication (SP) 800-160, Volume 2, focuses on cyber resiliency engineering—a specialty systems engineering discipline applied in conjunction with resilience engineering and systems security engineering to develop more survivable, trustworthy systems. Cyber resiliency engineering intends to architect, design, develop, maintain, and sustain the trustworthiness of systems with the capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources. From a risk management perspective, cyber resiliency is intended to reduce the mission, business, organizational, or sector risk of depending on cyber resources. This framework defines 'cyber resiliency' as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

CERT Resilience Management Model (CERT-RMM)[73]: The CERT Resilience Management Model (CERT-RMM), developed by the Software Engineering Institute (SEI) at Carnegie Mellon University, is the foundation for a process improvement approach to operational resilience management.

---

[71] "Alert (TA17-181A) Petya Ransomware," CISA, Revised February 15, 2018, https://www.cisa.gov/uscert/ncas/alerts/TA17-181A.

[72] NIST, SP 800-160 Volume 2 Revision 1: "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," December 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

[73] "CERT Resilience Management Model Collection (CERT-RMM)," Carnegie Mellon University Software Engineering Institute, accessed July 5, 2022, https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=514489.

Cybersecurity Capability Maturity Model (C2M2)[74]: The C2M2 is a free tool based on the CERT-RMM[75] and enables organizations to voluntarily measure the maturity of their cybersecurity capabilities. The C2M2 can help organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. The C2M2 focuses on the implementation and management of cybersecurity practices associated with information, IT, and OT assets and the environments in which they operate. The Department of Energy developed the C2M2 with the SEI in partnership with industry representatives.

Cyber Resilience Review (CRR)[76]: The CRR is also based on the CERT-RMM and is a free, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

Although the term "cyber" is used in both the Cyber Resilience Review and Cybersecurity Capability Maturity Model, it is not meant to limit the critical service or supporting assets in scope.

MITRE Cyber Resiliency Metrics[77]: MITRE's report provides a reference for systems engineers, program management staff, and others concerned with assessing or scoring cyber resiliency for systems and missions; selecting cyber resiliency metrics to support cyber resiliency assessment; and defining, evaluating, and using cyber resiliency measures of effectiveness (MOEs) for alternative cyber resiliency solutions. MITRE defines "cyber resiliency" for these metrics as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.

National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)[78]: The CAF collection encompasses a set of cyber security and resilience principles for securing essential services, a collection of supporting guidance, and a CAF incorporating indicators of good practice. The focus is on essential functions which if compromised could potentially cause significant damage to the economy, society, the environment, and individuals' welfare, including loss of life. The NCSC uses the term 'cyber resilience' in the CAF to refer to an organization's ability to

---

[74] "Cybersecurity Capability Maturity Model Version 2.1," U.S. DOE Office of Cybersecurity, Energy Security, and Emergency Response, June 2022, https://c2m2.doe.gov/.

[75] "CERT Resilience Management Model Collection (CERT-RMM)," Carnegie Mellon University Software Engineering Institute, accessed July 5, 2022, https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=514489.

[76] "Assessments: Cyber Resilience Review", CISA, accessed July 5, 2022, https://www.cisa.gov/uscert/resources/assessments.

[77] Deborah Bodeau et al., MITRE, Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods, September 2018, https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.

[78] "National Cyber Security Centre (NCSC) Cyber Assessment Framework Guidance," NCSC, accessed July 5, 2022, https://www.ncsc.gov.uk/collection/caf/introduction.

maintain the correct operation of its essential functions even in the presence of adverse cyber events and manage the risk of unacceptable consequences occurring because of a cyber-attack.

Resilience Metrics and Assessments: Conduct evaluations of the efficacy of operating practices with respect to resilience. DHS, NIST, and other federal agencies, and state regulatory authorities could:

- Scope a more concise and practical definition for resilience, and select or develop resilience metrics that incorporate IT/OT convergence;
- Recommend practices to enhance the efficacy of current planning and scenario criteria in addressing resilience;
- Conduct, coordinate, or sponsor an assessment of the critical infrastructure sectors and their interdependencies to identify areas where upgrades, modifications to operating procedures, or additional protective or adaptive measures may be needed and recommend actions as appropriate; and
- Identify areas where additional and extraordinary costs may have to be incurred and evaluate whether cost-recovery mechanisms and regulatory support may be warranted.

Incentivizing research and development of protection, analytical and mitigation tools: Develop tools to improve resilience, to include robust system modeling scenarios of potential structured events, to assess system response capability where IT and OT people, processes, systems, and technology are integrated. These tools should include enhanced forensics and monitoring capabilities, tools, and protocols to allow for the graceful degradation of operational systems. Additional consideration should be given to the potential for operating the system for extended periods without critical elements. Also, guidelines could be developed or improved on how to monitor systems, such as engineering workstations, that bridge IT and OT networks, to detect and uncover disruptions or threat actors more quickly.

1.6. Changing Our Mindset to Think Like an Adversary

IT/OT cyber-attacks capable of impacting operational processes or equipment require the attacker to understand the automation process and engineering design of the operational systems in detail. This knowledge enables the attacker to cause desired effects on systems in ways that circumvent or impact safety mechanisms to achieve a cyber-physical attack rather than an IT attack that unintentionally impacts OT systems. Cyber security standards and frameworks, whether for IT or OT systems, are foundational to protecting systems. However, they are not designed to protect against advanced persistent threats (APT) who have conducted extensive reconnaissance to understand the automation process and engineering design of the targeted OT systems. Even government advisories describing observed APT tactics, techniques, and procedures can get lost in the sea of alerts, advisories, vulnerability announcements, that are released with overwhelming frequency.

Many organizations are conditioned to having a defensive or even a regulatory-compliant mindset. They can get lost in trying to make sense of each alert and advisory and devote their resources to improving defensive perimeters without recognizing the true nature of an APT, who can change their tactics, techniques, and

procedures to circumvent perimeter security. Cybersecurity standards and frameworks along with perimeter security measures are very important for cyber hygiene. However, simply complying with standards or a framework may lead an organization to believe that they are adequately protected from an APT. Organizations must also factor in increasing IT/OT convergence, as an APT could intentionally or unintentionally use the integration to impact operational systems. The following are several types of models and methodologies that exist to help an organization think like the adversary and improve their defenses.

Cyber Kill Chain®: The Cyber Kill Chain® was designed to leverage knowledge about APTs to create an intelligence feedback loop to enable defenders to better detect and respond to adversary intrusions. The kill chain model shows defenders the phases of intrusions, maps adversary kill chain indicators to defender courses of action, identifies patterns that link individual intrusions into broader campaigns, and helps defenders understand the iterative nature of intelligence gathering. As defenders better understand the attackers' process, the defenders can better plan their network defense, response, and resource prioritization.[79]

Industrial Control Systems (ICS) Cyber Kill Chain: The ICS Cyber Kill Chain expands on the Cyber Kill Chain® model to circumvent or impact safety systems for a cyber-physical attack, not just an attack characterized as espionage, ICS disruption or intellectual property theft.[80]

Design Basis Threat (DBT): A DBT is the threat assessment, focused on both insider and external threats, usually associated with nuclear security requirements for nuclear or other radioactive material and associated facilities[81].

MITRE's Systems Engineering for Mission Assurance[82]: The goal of engineering for mission assurance is a system that is resilient enough to repel an intentional or accident failure or changes that may occur due to the environment. It allows for the systems to continue to function as intended safely and securely even during a cyber or physical attack that may occur internally or externally. Mission Assurance includes Cyber Mission Assurance, Crown Jewels Analysis, Cyber Threat Susceptibility Assessment, and Cyber Risk Remediation Analysis. Cyber Mission Assurance uses the concept that the system architecture is resilient when encountering cyber threats. Crown Jewel Analysis provides the defender with the knowledge of what is most critical to the mission as the assets are identified and cataloged. Because protecting all assets at the same security level to defend against an almost endless list of attack scenarios would be too costly, the Crown Jewel Analysis allows system engineers, designers, and operators to prioritize their efforts on critical systems to improve their resilience during an attack. Cyber Threat Susceptibility Assessment provides a method for the defender to understand the threats

---

[79] Rohan Amin, Michael Clopperty, and Eric Hutchins, Lockheed Martin Corporation (Corp.), "Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," accessed July 5, 2022, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[80] Michael Assante and Robert Lee, SANS Institute, "The Industrial Control System (ICS) Cyber Kill Chain," October 2015, https://www.sans.org/white-papers/36297/.

[81] International Atomic Energy Agency, "Design Basis Threat," accessed July 5, 2022, https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material/design-basis-threat.

[82] MITRE, "Cyber Mission Assurance Engineering: A Risk-Based, Threat-Informed Approach to Address Advanced Adversaries," June 2013, https://www.mitre.org/sites/default/files/publications/cyber-mae.pdf.

and the underlying risks to the assets that were identified using the Crown Jewel Analysis. Finally, Cyber Risk Remediation Analysis is applied to the identified assets to apply mitigation measures as required to defend the system.

INL's Consequence-driven, Cyber-informed Engineering (CCE): CCE is a think-like-the-adversary approach to cybersecurity that aims to reduce the impact of an advanced, targeted cyber sabotage campaign on an organization's most critical operations. Assuming an aggressor mindset, CCE examines how an adversary might target the most critical operations, focusing on entire systems and processes, not individual technologies. Rather than focusing on perimeter defenses that reduce attacker access, CCE results in engineering changes and process improvements that limit the damage an attacker can do once inside. CCE is considered consequence-driven because executives and operational experts identify the most critical functions essential to fulfilling their organization's mission and determine the potential consequences of a cyberattack against these functions. It is cyber-informed because system operators identify key points within a critical system vulnerable to a cyberattack. The methodology then leverages an organization's operational expertise, system understanding and process knowledge to engineer out cybersecurity risks.

There are four phases in CCE; Phase 1 is Consequence Prioritization: Sets a clear focus on the risk management framework to select operations that must not fail and associated attack scenarios that could bring them down. Phase 2 is System of Systems Analysis: Gathers information and identifies the systematic interdependencies between critical processes, defense systems, and enabling or dependent components. Phase 3 is Consequence-Based Targeting: Determines the adversary's path to achieve the highest impact effects, where they need to be to conduct the attack, and what information is required to achieve those goals. Phase 4 is Mitigations and Protections: Removes or disrupts the digital attack paths as fully as possible.

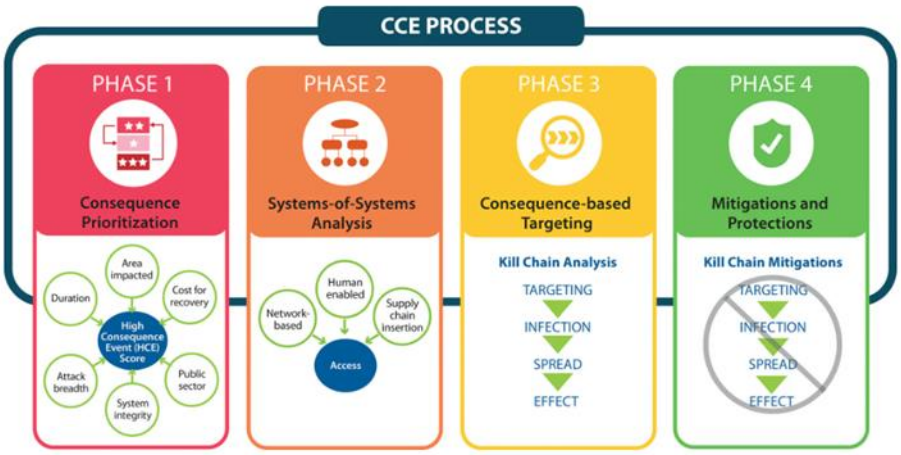

Figure 3: Consequence-driven Cyber-informed Engineering Process[83]

[83] Idaho National Laboratory, "Consequence-Driven Cyber-Informed Engineering," accessed July 1, 2022, https://inl.gov/cce/.

The methodology acknowledges the risks of internet-connected technology and services. In addition to relying on traditional protection strategies like intrusion detection software or additional firewalls, CCE uses engineering design principles to prevent APTs from damaging or disrupting utilities' most essential operations.

1.7. Personnel Training on Breach/Incident Response

There is a plethora of references and information focusing on the training and awareness for users related to cyber–Incident Response and Recovery (IRR). This training helps the user recognize attacks like a spear phish and what actions or notifications they should perform. Specifically, for OT environments some sectors require special training for the operators to help them recognize activity that may be an indicator of a cyberattack. For incident response there is also volumes of information on what processes to follow and how to understand an attacker's methodology. The Cyber Kill Chain®[84] and MITRE ATT&CK®[85] are two examples of information that will help guide an incident responder to better understand the attack process. It should not be assumed the incident responder is well trained at a company, because attacks in the OT environment do not appear to be as frequent as the IT environment, and staff may become stale with their skills or never have actually responded to a cyberattack and therefore will be learning as they go through the remediation and recovery process, which is never good. The Federal Energy Regulatory Committee, in partnership with the North American Electric Reliability Committee and the Regional Entities, interviewed eight electric sector utilities specific to how their OT performs IRR. The report presented several observations such as, the importance of knowledgeable IRR staff, exercising the IRR Plan, and having consistent plans across the entire organization.[86]

Before understanding what is required to respond to a breach it is important to define the terminology, in order that personnel know what is meant by terms such as "incident" and "event."

"*Organizing an effective computer security incident response capability (CSIRC) involves several major decisions and actions. One of the first considerations should be to create an organization-specific definition of the term 'incident' so that the scope of the term is clear. The organization should decide what services the incident response team should provide, consider which team structures and models can provide those services, and select and implement one or more incident response teams. Incident response plan, policy, and procedure creation is an important part of establishing a team, so that incident response is performed effectively, efficiently, and consistently, and so that the team is empowered to do what needs to be done. The plan, policies, and procedures should reflect the team's interactions with other teams within the organization as well as with outside parties, such as law enforcement, the media, and other incident response organizations.*"[87] Additionally

---

[84] Amin, Clopperty, and Hutchins,, Lockheed Martin Corporation (Corp.), "Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,"

[85] "ATT&CK," MITRE, accessed July 5, 2022, https://attack.mitre.org/.

[86] FERC, North American Electric Reliability Corporation (NERC), and Regional Entities, "Cyber Planning for Response and Recovery Study," September 2020, https://www.ferc.gov/sites/default/files/2020-09/FERC%26NERC_CYPRES_Report.pdf.

[87] NIST, Special Publication (SP) 800-61 Revision. 2: "Computer Security Incident Handling Guide," August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

the company should also develop a definition for the term 'event' since a suspicious event is typically initially treated as an event. An event may escalate to an incident after the security team examines the malicious activity.

Critical infrastructure companies with OT environments have revealed most companies define an event and incident slightly differently, this is partially a response to regulation and compliance. There does not appear to be a correlation between company, size, function, or geographic location as to how these definitions varied. However, there was a correlation between how these definitions were defined in relation to the scope of the IRR Plan. It is also important to note the companies also varied on what conditions would trigger the IRR Plan. The companies referred to the IRR Plan when an actual incident was determined but often referred to a "Cyber Event Plan" to address preliminary unknown issues, escalating the event through a documented process until a threshold of incident was determined. This escalation process was triggered by their definition of incident as well as the risk level of the environment in which the event occurred. It is important to understand when an event becomes an incident and when outside help may be needed, thus the importance of definitions.

Today's attack landscape can no longer be thought of as operating system or platform specific. Malicious code is written in cross-platform languages such as Java. Attacks can be sophisticated and quick, unfortunately a responder may only have hours to identify and isolate an attack conducted by a knowledgeable adversary. An IRR Plan puts structure around how the company implements its cybersecurity strategy with its business strategy and responds to an incident that could operationally and/or financially damage a company. To keep pace with challenges of the threat environment the IRR Plan should address some of these key aspects for each phase of the incident response cycle, Figure 4:

- Leadership support allows for the delegation of authorities as needed as well as funding support for the IRR team, communication, training, and tools to maintain a robust IRR process.
- Clear and concise mission statement and support service guidelines to prevent mission creep.
- Definition of an event and incident will steer the response team to a determination of escalation and the company should have a strong working knowledge of the incident response process from early detection to post incident activity.
- A core team that understands the process, is technically strong, and has a clear line of authority to make decisions based on certain conditions.
- Documented processes to include Event Plans and IRR Plans that should be continually evaluated, tested, and improved upon. This includes evaluating personnel (internal and external), security training, hardware, software, relationships, and processes and procedures.
- Legal authorities allow for actions such as gathering information, coordinating with internal and external parties, and sharing of information to assist in the response and recovery process.
- Understand what aspects of the system contain sensitive information and protect accordingly, ensure there is a protocol in place to share and release sensitive information as needed to respond and recover.

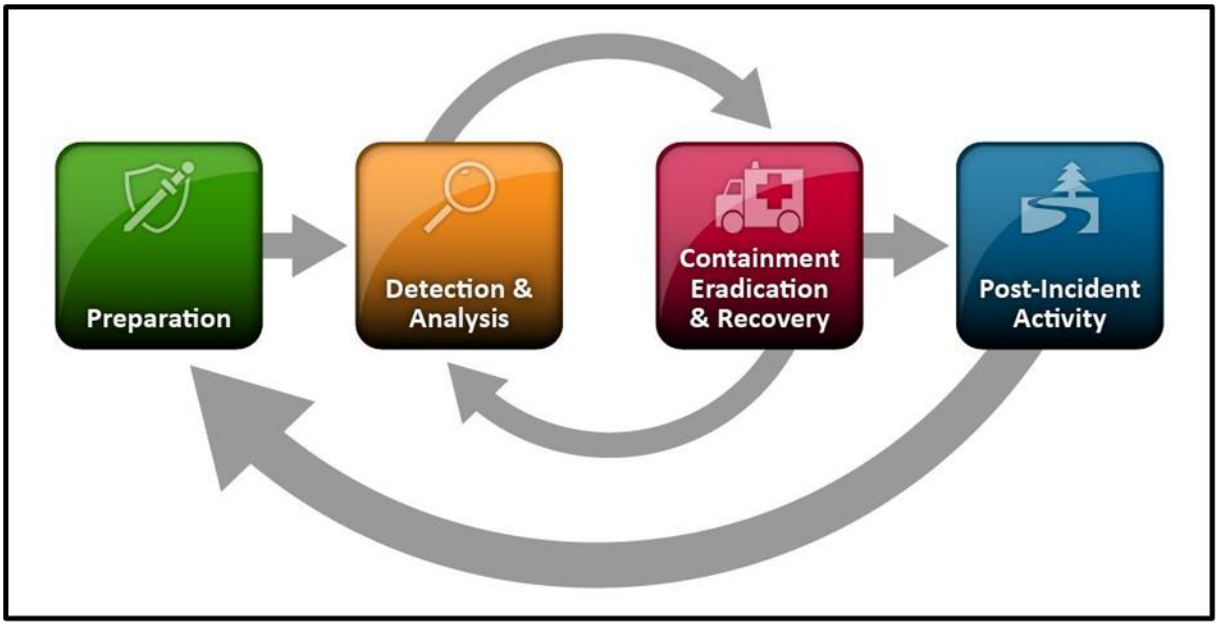

Figure 4: The Incident Response Cycle[88]

The shortage of skilled cyber staff, to include both IT and OT security continues to impede progress. It is estimated *"only 68 qualified workers are available for every 100 cybersecurity jobs, and over 600,000 jobs open up for cybersecurity workers every year in the U.S."*[89] This number is not expected to reduce anytime soon. Unfortunately, the critical sectors are not immune to the shortage and compete for cyber resources with all the other sectors. However, making it even more difficult they additionally look for cybersecurity staff that understand the OT environment and ICS.

The importance of frequently testing an IRR plan cannot be overstated. An incident that reaches phase six or seven of the Cyber Kill Chain is not common in the OT environment, or at least it is not being reported. As a result, company cybersecurity staff that work in the OT environment may have little to no experience responding to a complicated attack where the attacker is deeply embedded in the OT environment. Exercising the IRR Plan with realistic attack scenarios that consider a complex compromise that is deep into the Cyber Kill Chain will expose operating conditions that may not have been considered if only training to a single device compromise or small cluster of devices. Using real world examples to test the IRR Plan is a best practice. For example, use the SolarWinds Supply Chain Attack[90] but substituting required ICS equipment as the compromised equipment. Test the IRR Plan as if the compromise reached phase seven, Actions on Objectives, of the Cyber Kill Chain. Consider what happens to the environment if equipment and replacement equipment is unavailable for extended periods,

---

[88] NIST, "Computer Security Incident Handling Guide"

[89] Tim Hatton,"The Cybersecurity Talent Shortage," Emsi, March 8, 2022, https://www.economicmodeling.com/2022/03/08/the-cybersecurity-talent-shortage/.

[90] Mandiant, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," December 13, 2020, https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

remove key personnel are unable to participate to include key decision makers, and plan as if the event lasts for weeks. For example, every PLC running the water system from vendor XXX has a logic bomb that will disable all the devices within four hours, the attacker has established a covert command that has been in place for over a year, and Active Directory is compromised with Domain Admin Rights, allowing for the creation of authorized accounts by the attacker. Lastly, this was first discovered at 0130 Sunday morning. How do you respond?

An OT compromise that reaches phase seven of the Cyber Kill Chain is not common, because of this fact even well-trained staff may lose their skill over time since they are not utilizing their expertise. It is important for a company to recognize they need to constantly train their staff and may need to bring in outside assistance to help eradicate the attacker. A company must be familiar with their IRR Plan, and it needs to be detailed. It is common for a company to have separate IRR plans for their IT and OT environment. It is also common for a regulated company to have an additional IRR Plan simply to meet regulatory requirements. Citing the CYPRES Report,[91] it was discovered that a utility using a single or similar IRR Plan between the IT and OT environments may provide a better understanding of the IRR process across the company.

Another important aspect of IRR that staff understand both the IT and the OT environments and their operational differences. While IT IRR staff may not anticipate responding to an event in the OT environment, there may be reasons for them to understand the OT environment, below are a few.

1) The convergence of IT and OT make some of these systems ubiquitous and the IT IRR staff may have a better understanding of the device but not how it may interact with the OT environment.

2) IT staff may have to perform response and recovery on OT equipment.

3) Importance of understanding the architecture and design so they do not have to learn on the fly during an event or make a mistake of connecting a system or using protocols.

4) Understanding the devices in the OT environment may send flow and security data to the NOC and SOC, which is managed by IT.

5) Knowing who their OT staff counterparts are, meeting them for the first time during an event will slow recovery.

6) Consistent training across environments.

7) Understand the impact of removing a device from the network, i.e., sometimes an OT device may not simply be shut down and removed because it will impact the safety of the environment.

There are many government resources available to help a company with IRR. Below is a very short list.

[91] FERC, NERC, and Regional Entities, "Cyber Planning for Response and Recovery Study"

SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC (nist.gov)

Incident Response Training | CISA

Critical Infrastructure Exercises | CISA

1.8. Recommendations for asset owners

1) Not only provide security awareness to all staff but also provide frequent training to incident response staff so they remain fresh. Train IT staff so they understand the OT environment.

2) Test the IRR Plan frequently with complex real-world scenarios, this will help stuff remain fresh as well as identify gaps in the IRR Plan and security.

3) Be prepared to ask for help outside the organization if a breach occurs.

4) Utilize outside resources to prepare and maintain a robust IRR Plan. i.e., NIST, DHS, and private sector organizations that specialize in IRR.

5) Develop IRR plans that are consistent across environments, such as the IT and OT. This includes consistent definitions.

Appendix G. Membership and Participants

Table 1: Subcommittee Leadership

Name	Organization	Role
Mr. Jack Huffard	Tenable Holdings, Inc.	Subcommittee Chair
Mr. Jamie Brown	Tenable Holdings, Inc.	Working Group Co-Lead
Mr. Marty Edwards	Tenable Holdings, Inc.	Working Group Co-Lead

Table 2: Subcommittee Membership

Name	Organization
Mr. Drew Batten	Cybersecurity and Infrastructure Security Agency (CISA)
Mr. Brad Behm	Amazon Web Services, Inc.
Mr. Christopher Boyer	AT&T, Inc.
Mr. Christopher Day	Tenable Holdings, Inc.
Ms. Patricia Eke	Microsoft Corp.
Mr. Grant Geyer	Claroty
Ms. Katherine Gronberg	NightDragon Security, LLC
Mr. Daryl Haegley	U.S. Department of Defense (DoD)
Mr. Robert Hoffman	Broadcom, Inc.
Mr. Andrew Howell	Operational Technology Cybersecurity Coalition
Mr. Barry Kuehnle	U.S. Federal Energy Regulatory Commission (FERC)
Mr. Kent Landfield	Trellix
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Richard Mosley	AT&T, Inc.
Mr. Thomas Patterson	Unisys Corp.
Mr. Alex Reniers	CISA

Name	Organization
Mr. Del Rodillas	Palo Alto Networks, Inc.
Mr. Nicholas Seeley	Schweitzer Engineer Laboratories
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Robert Spiger	Microsoft Corp.
Dr. Claire Vishik	Intel Corp.

Table 3: Briefers, Subject-Matter Experts

Name	Organization
Mr. Brad Behm	Amazon Web Services, Inc.
Mr. Jim Beardsley	Nuclear Regulatory Commission
Mr. Jeff Cornelius	Darktrace
Mr. Michael Dransfield	National Security Agency
Dr. Allen Friedman	CISA
Mr. James Goosby	Southern Company
Mr. Daryl Haegley	DoD
Mr. Darren Highfill	Norfolk Southern Corp.
Mr. Matt Hyatt	Georgia Systems Operations Corp.
Mr. Michael Keane	FERC
Mr. Stu Kippleman	Parsons
Ms. Sharon Koller	American Transmission Co.
Mr. Robert Lee	Dragos
Mr. Ariel Levite	CEIP
Ms. Kate Marks	U.S. Department of Energy
Mr. Kevin Morley	American Water Works Association

Name	Organization
Ms. Sandra Parker	Dow
Mr. Jitendra Patel	AT&T, Inc.
Mr. Scott Quenneville	American Transmission Co.
Mr. Alex Reniers	CISA
Mr. Del Rodillas	Palo Alto Networks, Inc.
Ms. Megan Samford	Schneider Electric
Ms. Elke Sobieraj	National Security Council
Mr. Jake Young	Microsoft
Ms. Amy Zwarico	AT&T, Inc.

Table 4: Subcommittee Management

Name	Organization
Ms. DeShelle Cleghorn	President's National Security Telecommunications Advisory Committee (NSTAC) Alternate Designated Federal Officer (ADFO)
Mr. Scott Zigler	NSTAC ADFO
Mr. Santana King	Teksynap Corp.
Ms. Laura Penn	Edgesource Corp.
Ms. Shiri Telfer	Edgesource Corp.

Appendix H. Acronyms

Table 5: Acronyms

Acronym	Definition
4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
ADFO	Alternate Designated Federal Officer
AI/ML	Artificial Intelligence and Machine Learning
BOD	Binding Operational Directive
CI	Critical Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CNSSI	Committee on National Security Systems Instruction
CSP	Cloud Service Provider
CSWG	Control Systems Working Group
CUI	Controlled Unclassified Information
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
EO	Executive Order
FERC	U.S. Federal Energy Regulatory Commission
FBI	U.S. Federal Bureau of Investigation
GCC	Government Coordinating Councils
IAM	Identity and Access Management
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission

Acronym	Definition
IIJA	Infrastructure Investment and Jobs Act
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
LoRa	Long-Range
LTE	Long-Term Evolution
MOA	Memorandum of Agreement
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
NSA	National Security Agency
NSM	National Security Memorandum
NSPD	National Security Presidential Directive
NSTAC	President's National Security Telecommunications Advisory Committee
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OT	Operational Technology
PLC	Programmable Logic Controllers
SaaS	Software-as-a-Service
SCC	Sector Coordinating Councils
SI	Systems Integrator
SOC	Security Operations Center
SLTT	State, Local, Tribal, and Territorial

Acronym	Definition
SP	Special Publication
SSH	Secure Shell Protocol
U.S.	United States
U.S.C.	United States Code
USG	United States Government
ZTA	Zero Trust Architecture

Appendix I. Definitions

Table 6: Definitions

Term	Definition	Source
Active Directory	A Microsoft directory service for managing identities in Windows domain networks (registered trademark).	▪ National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-16B NIST SP 1800-16C NIST SP 1800-16D
Adversary	Any individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.	▪ NIST SP 800-30
Artificial Intelligence	(1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. (2) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.	▪ American National Standards Institute International Committee for Information Technology Standards 172-220 (R2007) Information Technology -- American National Standard Dictionary of Information Technology ▪ Cited in NIST's *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	▪ National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 8006 under "cloud computing"

Term	Definition	Source
Connectivity	Capacity for interconnecting platforms, systems, and applications.	▪ PCMag, https://www.pcmag.com/encyclopedia/term/connectivity
Controlled Unclassified Information	Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under *EO 13526: Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.	▪ NIST SP 800-171 Rev. 2 under controlled unclassified information from EO 13556 ▪ NIST SP 800-172 under controlled unclassified information from EO 13556 ▪ NIST SP 800-171 Rev. 1 [Superseded] under controlled unclassified information from EO 13556
Counterfeit	An unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source.	▪ NIST SP 800-161, 18 United States Code (U.S.C.)
Critical Infrastructure	Sixteen sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.	▪ Cybersecurity Infrastructure Security Agency, https://www.cisa.gov/critical-infrastructure-sectors

Term	Definition	Source
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.	▪ Committee on National Security Systems Instruction (CNSSI) 4009-2015 from National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23) ▪ NIST SP 1800-25B under Cybersecurity from CNSSI 4009-2015 ▪ NSPD-54/HSPD-23 ▪ NIST SP 1800-26B under Cybersecurity from CNSSI 4009-2015 ▪ NSPD-54/HSPD-23 ▪ NIST SP 800-160 Vol. 2 from CNSSI 4009-2015 ▪ NIST SP 800-37 Rev. 2 ▪ NIST SP 800-53 Rev. 5 from OMB Circular A-130 (2016) ▪ NISTIR 7621 Rev. 1 under Cybersecurity from CNSSI 4009-2015
Directory Services	A distributed database service capable of storing information, such as certificates and certificate revocation lists, in various nodes or servers distributed across a network. (In the context of this practice guide, a directory services stores identity information and enables the authentication and identification of people and machines.)	▪ NIST SP 1800-16B under Directory Service from NIST SP 800-15 ▪ NIST SP 1800-16D under Directory Service from NIST SP 800-15

Term	Definition	Source
Emerging Technologies	Technologies that are currently developing and are expected to impact society in some significant way over the next 5 to 10 years.	▪ Independence University, https://www.independence.edu/blog/what-is-emerging-technology
EO 14028, Improving the Nation's Cybersecurity	Charges multiple agencies, including NIST, with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.	▪ Federal Register: Improving the Nation's Cybersecurity
Fifth Generation	The fifth installment of advanced wireless technology, bringing about increased bandwidth and capacity for advancements within the Internet of Things.	▪ Qualcomm, https://www.qualcomm.com/5g/what-is-5g
Fourth Generation (4G)	A successor of the third-generation standards. A 4G system provides mobile ultra-broadband internet access, for example to laptops with Universal Serial Bus wireless modems, to smartphones, and to other mobile devices.	▪ International Center for Applied Studies in IT, http://icasit.gmu.edu/course-databases/technology-topics/4g-technology/
Hardware	The physical components of an information system.	▪ NIST SP 800-53 Rev. 4 under Hardware CNSSI 4009
Identity and Access Management	(Also known as identity management.) A fundamental cybersecurity concept focused on ensuring "the right people and things have the right access to the right [technology] resources at the right time."	▪ NIST: Identity and Access Management, https://www.nist.gov/identity-access-management

Term	Definition	Source
Industrial Control System (ICS)	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy)	▪ NIST, https://csrc.nist.gov/glossary/term/industrial_control_system
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.	▪ Federal Information Processing Standards 200 under Information Technology 40 U.S.C., Sec. 1401

Term	Definition	Source
Infrastructure Investment and Jobs Act	Requires brokers to report to the Internal Revenue Service the cost basis of digital assets transferred by their clients to non-brokers, similar to how securities brokers report stock and bond trades.	▪ Small Business Association of Michigan, https://www.sbam.org/the-infrastructure-investment-and-jobs-act-includes-tax-related-provisions-youll-want-to-know-about/
Internet of Things	Internet of Things (IoT) refers to systems that involve computation, sensing, communication, and actuation (as presented in NIST SP 800-183). IoT involves the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision making.	▪ NIST SP 800-183
Long-Term Evolution	Long-Term Evolution (LTE), commonly referred to as 4G, is a standard for nationwide public safety broadband. This standard allows access to digital technologies and deliver expanded capabilities in the field. The LTE standard supports fast speeds, with speeds up to 10 times faster than 3G networks.	▪ NIST, U.S. Department of Justice
Machine Learning	A branch of artificial intelligence focused on building applications that learn from data and improve their accuracy over time without being programmed to do so.	▪ IBM, https://www.ibm.com/cloud/learn/machine-learning
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.	▪ CNSSI 4009-2015 under malicious logic from Internet Engineering Task Force Request for Comments 4949 V2

Term	Definition	Source
National Security and Emergency Preparedness	Policies, plans, procedures, and readiness measures that enhance the ability of the U.S. government to mobilize for, respond to, and recover from a national security emergency.	▪ Department of the Interior, https://www.doi.gov/sites/doi.gov/files/-900-dm-5-nsep-2021.pdf
National Vulnerability Database (NVD)	The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.	▪ NIST, https://nvd.nist.gov/
Operating System	The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.	▪ NIST SP 800-44 Version 2 ▪ NISTIR 7621 Rev. 1 from NIST SP 800-44 Version 2

Term	Definition	Source
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.	▪ NIST SP 800-37 Rev. 2
Protocol	A set of rules governing the exchange or transmission of data between devices.	▪ Britannica, https://www.britannica.com/technology/protocol-computer-science
Sixth Generation	Sixth generation of wide-area wireless technology.	▪ PCMag, https://www.pcmag.com/news/what-is-6g

Term	Definition	Source
Software Application	A software program hosted by an information system.	▪ CNSSI 4009-2015 from NIST SP 800-37 Rev. 1 ▪ NIST SP 1800-16B under Application from NIST SP 800-137 ▪ NIST SP 1800-16C under Application from NIST SP 800-137 ▪ NIST SP 1800-16D under Application from NIST SP 800-137 ▪ NIST SP 800-137 under Application from NISTIR 7298 ▪ NIST SP 800-37 Rev. 2 ▪ NIST SP 800-53 Rev. 5 from NIST SP 800-37 Rev. 2 ▪ NISTIR 7621 Rev. 1 under Application from CNSSI 4009-2015 ▪ NIST SP 800-37 Rev. 1 [Superseded] under Application
Software Developers	A person or group that designs and/or builds and/or documents and/or configures the hardware and/or software of computerized systems.	▪ Food and Drug Administration, Glossary of Computer System Software Development Terminology (8/95)
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or DoS.	▪ NIST SP 800- 53, CNSSI 4009, Adapted

Term	Definition	Source
Threat Environment	The online space where cyber threat actors conduct malicious cyber threat activity.	▪ An Introduction to the Cyber Threat Environment, https://icclr.org/wp-content/uploads/2019/05/Intro-to-cyber-threat-environment-e.pdf?x37853
Trustworthiness	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.	▪ NIST SP 800-39, CNSSI-4009
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).	▪ NIST SP 800-161 under Verification from CNSSI 4009 ▪ ISO 9000 – Adapted ▪ NISTIR 7622 under Verification from CNSSI 4009, ISO 9000 – Adapted
Virtual Private Network	A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.	▪ NIST SP 800-113 under Virtual Private Network
Zero Trust	A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.	▪ NIST SP 800-207, https://doi.org/10.6028/NIST.SP.800-207

Term	Definition	Source
Zero Trust Architecture	An architecture that treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized.	▪ NIST, https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

Appendix J. Bibliography

Amazon Web Services. "Security Best Practices for Manufacturing Operational Technology (OT)," May 2021. https://d1.awsstatic.com/whitepapers/security-bp-for-manufacturing-ot.pdf.

Amin, Rohan, Clopperty, Michael, Hutchins, Eric, and the Lockheed Martin Corporation (Corp.). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Accessed July 5, 2022. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

Assante, Michael and Lee, Robert, and The SANS Institute. "The Industrial Control System (ICS) Cyber Kill Chain," October 2015. https://sansorg.egnyte.com/dl/HHa9fCekmc.

Beardsley, Jim, U.S. Nuclear Regulatory Commission (NRC). "U.S. NRC Cyber Security for Power Reactors," Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Information Technology (IT) and OT Convergence Subcommittee, Arlington, VA, March 15, 2022.

Behm, Brad, Amazon Web Services. "IT/OT Convergence from Amazon's Perspective," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 26, 2022.

Bisson, David. "NotPetya: Timeline of a Ransomworm," Tripwire.com, June 28, 2017.https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/.

Bochman, Andrew, Idaho National Laboratory. "Engineering Out Cyber Risk," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, June 2, 2022.

Bodeau, Deborah, Graubert, Richard D., McQuaid, Rosalie M., Woodill, John, and MITRE. "Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods," September 2018. https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.

Borgne, Sophie. "IT/OT Convergence in the New World of Digital Industries," Schneider Electric (blog), April 13, 2021, https://blog.se.com/sustainability/2021/04/13/it-ot-convergence-in-the-new-world-of-digital-industries/.

Brubaker, Nathan, Caba, Dan, Glyer, Christopher, Johnson, Blake, Krotofil, Marina, Scali, Dan,, and Mandiant. "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure," Mandiant.com, December 14, 2017. https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton.

Carnegie Mellon University Software Engineering Institute. "CERT Resilience Management Model Collection," sei.cmu.edu, Accessed July 5, 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=514489.

Center for Internet Security (CIS). "CIS Critical Security Controls." cisecurity.org, Accessed July 13, 2022. https://www.cisecurity.org/controls

Christman, Jason, Johnson Controls. "Securing Building OT in a Converged Environment – A Manufacturer's Perspective," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, June 14, 2022.

Cornelius, Jeff, Darktrace. "Self-Learning Artificial Intelligence for IT/OT Security," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, May 26, 2022.

Cybersecurity and Infrastructure Security Agency (CISA). "Alert (AA20-205A) National Security Agency (NSA) and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems," cisa.gov, Revised October 24, 2020. https://www.cisa.gov/uscert/ncas/alerts/aa20-205a.

CISA. "Alert (TA17-181A) Petya Ransomware," cisa.gov, Revised February 15, 2018. https://www.cisa.gov/uscert/ncas/alerts/TA17-181A.

CISA. "Assessments: Cyber Resilience Review," cisa.gov, Accessed July 5, 2022. https://www.cisa.gov/uscert/resources/assessments.

CISA. "Chemical Sector Regulatory Authorities and Executive Orders," cisa.gov, Accessed July 1, 2022. https://www.cisa.gov/chemical-sector-regulatory-authorities-and-eos.

CISA. "Critical Infrastructure Exercises," cisa.gov, Accessed July 1, 2022. https://www.cisa.gov/critical-infrastructure-exercises.

CISA. "Incident Response Training," cisa.gov, Accessed July 1, 2022. https://www.cisa.gov/incident-response-training.

CISA. "Information and Communications Technology (ICT) Supply Chain Risk Management Task Force," cisa.gov, Accessed July 1, 2022. https://www.cisa.gov/ict-scrm-task-force.

CISA. "Malware Analysis Report-17-352-01 HatMan—Safety System Targeted Malware (Update B)," February 27, 2019. https://www.cisa.gov/uscert/sites/default/files/documents/MAR-17-352-01 HatMan - Safety System Targeted Malware %28Update B%29.pdf.

CISA. "Protected Critical Infrastructure Information Program," cisa.gov, Accessed July 13, 2022.https://www.cisa.gov/pcii-program.

CISA. National Security Agency, and Office of the Director of National Intelligence, "Potential Threat Vectors to 5G Infrastructure," 2021. https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf.

Computer Security Resource Center. "Glossary: Resilience," nist.gov, Accessed July 5, 2022. https://csrc.nist.gov/glossary/term/resilience.

Dransfield, Michael, NSA. "IT/OT Convergence," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, March 15, 2022.

Hatton, Tim. "The Cybersecurity Talent Shortage," Emsi, March 8, 2022. https://www.economicmodeling.com/2022/03/08/the-cybersecurity-talent-shortage/.

Edison Electric Institute. "Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk Version 2.0," May 2020. https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/EEI-Law---Model-Procurement-Contract-Language.pdf.

Eke, Patricia, Microsoft, U.S. Cybersecurity Regulation, July 2022.

Federal Energy Regulatory Committee (FERC) and NRC. "Memorandum of Agreement Between the U.S. NRC and the FERC," September 2015. https://www.nrc.gov/docs/ML1503/ ML15033A181.pdf.

FERC, North American Electric Reliability Corporation (NERC), and Regional Entities. "Cyber Planning for Response and Recovery Study," September 2020. https://cms.ferc.gov/sites/default/files/2020-09/FERC%26NERC_CYPRES_Report.pdf.

FERC. "Statement from FERC Chairman Richard Glick: Chairman Glick and Commissioner Clements Call for Examination of Mandatory Pipeline Cyber Standards in Wake of Colonial Pipeline Ransomware Incident," May 10, 2021. https://www.ferc.gov/news-events/news/statement-ferc-chairman-richard-glick-chairman-glick-and-commissioner-clements.

Friedman, Allan, CISA. "Software Transparency: Opportunities, Progress, and Future Directions," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, March 10, 2022.

Gautreaux, Kevin, FedEx Corp. "The Evolution of OT/Internet of Things (IoT) Security at FedEx," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, June 14, 2022.

Greene, Jeffrey, and Sobieraj, Elke, National Security Council (NSC), and Scott, Brian, Office of the National Cyber Director. "The Administration's Efforts to Safeguard Critical Infrastructure," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, March 3, 2022.

Goosby, James, Sothern Company. "IT/OT Convergence in Electric Utility Environments," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, May 3, 2022.

Haegley, Daryl, U.S. Department of Defense (DoD). "DoD Control Systems/Operational Technology Cybersecurity Progress," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, March 17, 2022.

Hanks, Andy, State of Montana. "Recommendations for Managing IT/OT Convergence Risks," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, June 2, 2022.

Highfill, Darren, Norfolk Southern Corp. "Security Implications of IT/OT Convergence," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 5, 2022.

Hoffman, Mike and Winston, Tom, and Dragos. "Recommendations Following the Colonial Pipeline Cyber Attack," Dragos.com (blog), May 11, 2021. https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/.

Hullings, Dean, Forescout Technologies. "IT/OT Convergence – Challenges are Never a Technology Issue," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, May 31, 2022.

Hyatt, Matt, Georgia System Operations Corp. "IT/OT Convergence for Utilities," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 19, 2022.

Idaho National Laboratory. "Consequence-Driven Cyber-Informed Engineering," inl.gov, Accessed July 1, 2022. https://inl.gov/cce/.

International Atomic Energy Agency. "Design Basis Threat," iaea.org, Accessed July 5, 2022. https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material/design-basis-threat.

International Society of Automation (ISA). "ISA/International Electrotechnical Commission 62443 Series of Standards: The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards," isa.org, Accessed July 13, 2022, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

Keane, Michael, FERC. "Federal Oversight of Electric Reliability," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 7, 2022.

Kippelman, Stuart, Parsons. "IT/OT Challenges and Opportunities," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 28, 2022.

Koller, Sharon and Quenneville, Scott, American Transmission Company. "NSTAC Briefing on IT/OT Convergence from an Electric Sector Perspective," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 19, 2022.

Lee, Robert, Dragos. "ICS Cyber Threat Landscape and Evolving Trends," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, May 17, 2022.

Levite, Ariel, Carnegie Endowment for International Peace. "Corporate and Governmental Steps to Enhance ICT Supply Chain Integrity: Trends, Implications, and Recommendations," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 21, 2022.

Mandiant. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," Mandiant.com, December 13, 2020. https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

Marks, Kate, U.S. Department of Energy (DOE). "Addressing Cyber Threats in the Energy Sector," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, March 22, 2022.

Mesa Associates, "Designing your Substations for Grid Resiliency," exacterinc.com, Accessed July 1, 2022. https://www.exacterinc.com/resources/uploaded/Brochures/Substation Resiliency - Jeff Keller Mesa Eng.pdf.

Miller, Steve and Reese, Evan, Mandiant. "A Totally Tubular Treatise on TRITON and TriStation," Mandiant.com, June 7, 2018, https://www.mandiant.com/resources/totally-tubular-treatise-triton-and-tristation.

MITRE." ATT&CK," mitre.org, Accessed July 5, 2022. https://attack.mitre.org/.

MITRE. "Cyber Mission Assurance Engineering: A Risk-Based, Threat-Informed Approach to Address Advanced Adversaries," June 2013. https://www.mitre.org/sites/default/files/publications/cyber-mae.pdf.

Monken, Jonathan and Smith, Maggie, "The Colonial Pipeline Hack Shows We Need a Better Federal Cybersecurity Ecosystem," Modern War Institute at West Point, June 1, 2021. https://mwi.usma.edu/the-colonial-pipeline-hack-shows-we-need-a-better-federal-cybersecurity-ecosystem/.

Morley, Kevin, American Water Works Association, Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, May 26, 2022

National Conference of State Legislatures. "Cybersecurity Legislation 2021," ncsl.org, January 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecuritylegislation-2021.aspx.

National Council of Information Sharing and Analysis Centers (ISAC). "National Council of ISACs", nationalisacs.org, Accessed July 1, 2022. https://www.nationalisacs.org/.

National Cyber Security Centre (NCSC). "NCSC Cyber Assessment Framework Guidance," ncsc.gov.uk, Accessed July 5, 2022. https://www.ncsc.gov.uk/collection/caf/introduction.

National Infrastructure Advisory Council. "Critical Infrastructure Resilience Final Report and Recommendations," September 2009. https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

National Institute of Standards and Technology (NIST). "Cybersecurity Framework," nist.gov, Accessed July 1, 2022. https://www.nist.gov/cyberframework.

NIST. "Special Publication (SP) 800-61 Revision. 2: Computer Security Incident Handling Guide," August 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

NIST. "SP 800-160 Volume 2 Revision 1: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," December 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

NIST. "SP 800-161 Revision 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," May 2022. https://doi.org/10.6028/NIST.SP.800-161r1.

NIST. "SP 800-207: Zero Trust Architecture," August 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final.

NIST, SP 1500-201: Framework for Cyber-Physical Systems: Volume 1, Overview, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

Nickerson, Scott, Federal Bureau of Investigations. "Cyber Based Threats Against Critical Infrastructure," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, June 21, 2022.

NERC. "CIP-013-1: Cyber Security - Supply Chain Risk Management," nerc.com, Accessed July 7, 2022. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf.

NERC. "Project 2016-02 Modifications to Critical Infrastructure Protection Standards," nerc.com, Accessed July 1, 2022. https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx

NERC. "Reliability Standards for the Bulk Electric Systems of North America," nerc.com, Updated May 13, 2022. https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf.

Office of Electricity. "Demand Response," energy.gov, Accessed July 1, 2022. https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/demand-response

Oleniczak, Kevin, AWS. "Using AWS IoT for Predictive Maintenance," aws.amazon.com (blog), June 28, 2022. https://aws.amazon.com/blogs/iot/using-aws-iot-for-predictive-maintenance/

Parker, Sandra, Dow. "IT/OT Convergence – A Security Point of View," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, April 12, 2022.

Patel, Jitendra and Zwarico, Amy, AT&T. "IT/OT Convergence: AT&T Perspective," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, May 10, 2022.

Preminger, Amir.. "NotPetya: Looking Back Three Years Later," claroty.com, June 30, 2020. https://claroty.com/2020/06/30/notpetya-looking-back-three-years-later/.

President's NSTAC. "NSTAC Report to the President on Zero Trust and Trusted Identity Management," February 2022. https://www.cisa.gov/nstac-publications.

Reniers, Alex, CISA. "CISA ICS Security Program Brief," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, March 8, 2022.

Rodillas, Del, Palo Alto Networks. "Zero Trust Architecture for Converged IT/OT Networks," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, May 12, 2022.

Samford, Megan, Schneider Electric. "NSTAC IT/OT Convergence Subcommittee Briefing," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, May 17, 2022.

Schachter, Cordell, U.S. Department of Transportation. "Obstacles to Implementing Baseline Security Controls in IT/OT Systems," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, March 24, 2022.

Seeley, Nicholas, Schweitzer Engineering Laboratories. "A Manufacturer's Perspective on the IT/OT Convergence in Critical Infrastructure," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, March 24, 2022.

Shodan. "Search Engine for the Internet of Everything," shodan.io, Accessed July 1, 2022. https://www.shodan.io/.

Society of Cable Telecommunications Engineers and International Society of Broadband Engineers. *Journal of Energy Management Volume 2 Number 2*, August 2017, https://www.nrel.gov/docs/fy17osti/69034.pdf.

Taft, JD, Pacific Northwest National Laboratory. "Electric Grid Resilience and Reliability for Grid Architecture," November 2017, https://gridarchitecture.pnnl.gov/media/advanced/Electric_Grid_Resilience_and_Reliability.pdf.

The White House. "Executive Order (EO) 14028: Improving the Nation's Cybersecurity," May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

The White House. "EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017. https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

The White House. "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems," July 28, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

The White House. "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Transportation Security Administration, Sensitive Security Information, tsa.gov, Accessed July 13, 2022. https://www.tsa.gov/for-industry/sensitive-security-information.

U.S. Bureau of Labor Statistics. "Labor Force Statistics from the Current Population Survey," bls.gov, Accessed July 1, 2022, https://www.bls.gov/cps/cpsaat18.htm.

U.S. Congress. Infrastructure Investment and Jobs Act, November 2021, https://www.congress.gov/bill/117th-congress/house-bill/3684

U.S. Congress, Public Law 117–103: Making Consolidated Appropriations for the Fiscal Year Ending September 30, 2022, and for Providing Emergency Assistance for the Situation in Ukraine, and for Other Purposes, March 15, 2022, https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf.

U.S. Cyberspace Solarium Commission. "Report," March 2020, https://www.solarium.gov/report.

U.S. Department of Defense (DoD). "DoD Control Systems Security Requirements Guide Version 1 Release 1," January 26, 2021. https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/Jan_26_Control_Systems_SRG.pdf.

U.S. Department of Homeland Security (DHS). "DHS: Cyber Security Procurement Language for Control Systems," September 2009. https://www.cisa.gov/uscert/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf.

U.S. DOE Directives Program Office of Management (MA-1.2). "Resilience," doe.gov, Accessed July 5, 2022. https://www.directives.doe.gov/terms_definitions/resilience.

U.S. DOE Office of Cybersecurity, Energy Security, and Emergency Response. "Cybersecurity Capability Maturity Model Version 2.1," June 2022. https://c2m2.doe.gov/.

U.S. DOE Office of Electricity. "Critical Electric Infrastructure Information Final Rule: Questions and Answers," energy.gov, May 15, 2020. https://www.energy.gov/oe/articles/critical-electric-infrastructure-information-final-rule-questions-and-answers.

U.S. DOE Office of Electricity. "Demand Response," energy.gov, Accessed July 18, 2022. https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/demand-response.

U.S. Department of State. "Bureau of Cyberspace and Digital Policy," state.gov, Accessed July 13, 2022. https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/.

U.S. Government Accountability Office. "CYBER INSURANCE: Action Needed to Assess Potential Federal Response to Catastrophic Attacks," June 2022. https://www.gao.gov/assets/gao-22-104256.pdf.

Young, Jake, Microsoft Corp. "Hacking with Physics: A study of IT/OT Convergence," Briefing to the NSTAC IT/OT Convergence Subcommittee, Arlington, VA, June 21, 2022.