OWL Cyber Defense

WHITE PAPER

Protecting Critical Infrastructure in the DoD Landscape

"Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin American society."

- U.S. Department of Homeland Security

Introduction

Critical infrastructure systems and facilities are the fundamental elements of modern society, providing the necessary basic services that form a foundation for nearly all other activities. While they may be primarily focused on their missions, defense installations, bases, and facilities are also supported by a variety of critical infrastructure and operational technology, from power generation and utilities to building automation and safety systems.

Just like in civilian society, attacks against critical infrastructure in the defense landscape can result in loss of power, contaminated drinking water, exposure of confidential information, interruptions to operations, and threats to the safety of personnel. A successful attack against defense critical infrastructure can also cripple a vital response element to the safety of the entire country.

The cybersecurity of defense, military, and government IT systems is generally well-governed under a variety of regulations and policy stipulations. However, this patchwork of regulatory guidance can make it difficult "to determine the most cost-effective, appropriate set of security controls, which if implemented and determined to be effective, would mitigate risk while complying with security requirements defined by applicable federal laws, Executive Orders, regulations, policies, directives, or standards (e.g., FISMA, OMB Circular A-130, HSPD-12, FIPS Publication 200)." [1]

Even if appropriate technologies are selected to secure the breadth of IT and defense systems in the U.S. Department of Defense (DoD), there is little available specific guidance for protecting critical infrastructure within the defense context. This, combined with the unique challenges of protecting critical infrastructure in general, has led to a lack of institutional knowledge and an inconsistency in cyber protections for critical infrastructure assets under the umbrella of the DoD.

This document includes an overview of critical infrastructure, the associated cybersecurity challenges including a background on industrial control system (ICS) security, and provides a synthesis of the most recent available guidance to secure critical infrastructure and the various supporting systems within a defense context. It is intended as a "best practice" primer for the cybersecurity of DoD critical infrastructure, and to provide a basic foundation of accumulated knowledge.

[1] *NIST Special Publication 800-53 Rev 4, page 12*

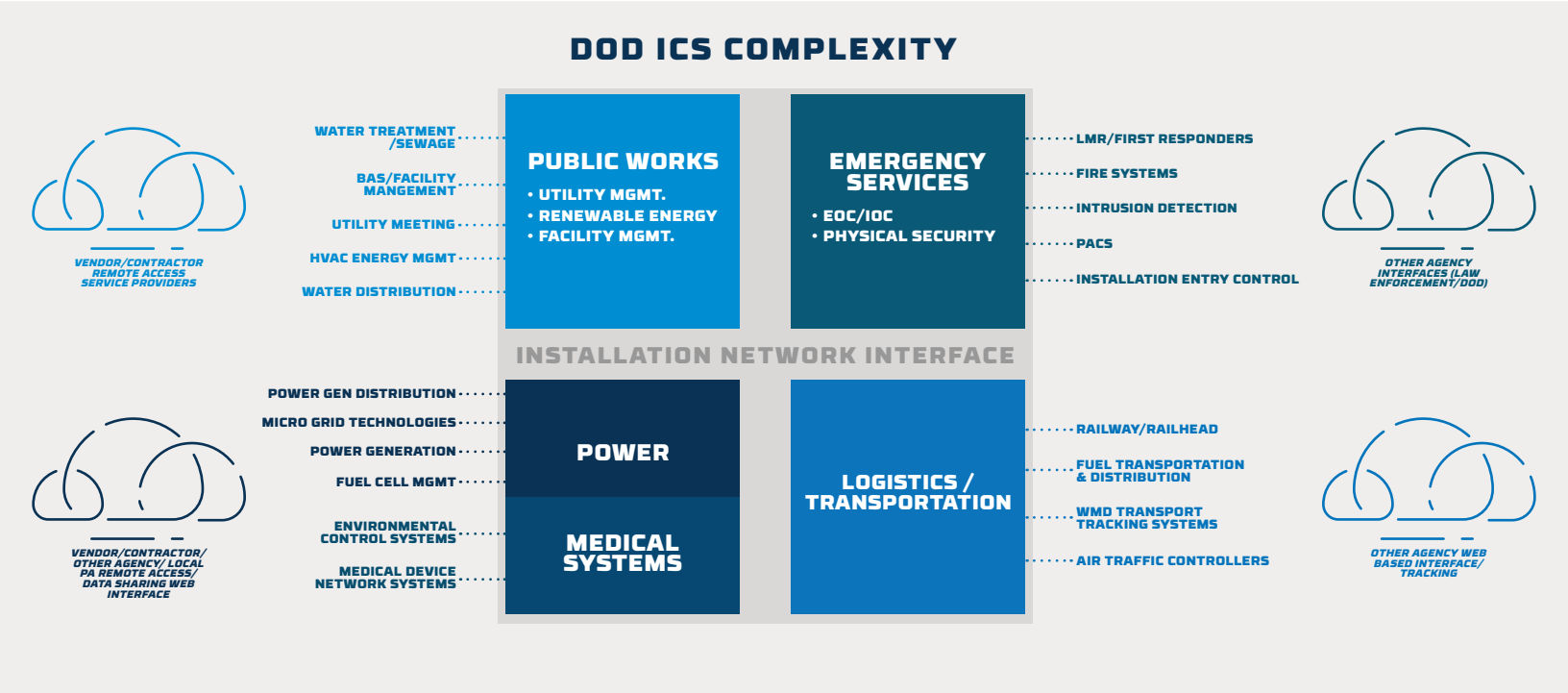
Overview

The National Infrastructure Protection Plan (NIPP) of 2013[2] designates the 16 specific sectors of critical infrastructure. These industry verticals contain assets and systems that are deemed so vital to the United States that their incapacitation or destruction would have a debilitating effect on the security, economy, national public health, or safety of the country. Critical infrastructure systems are not generally considered a direct part of military and defense information networks or infrastructure, but play critical supporting roles within the vehicles/ships, facilities, and field operations in the broad defense landscape.

The 16 Sectors of Critical Infrastructure

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

Obviously, not every sector of critical infrastructure applies to defense (e.g. financial services), but the U.S. Department of Defense remains one of the largest owners of critical infrastructure in the federal government, with more than 500 installations, 300,000 buildings, 250,000 linear structures, and over 2.5 million unique ICSs.[3] From nuclear reactors on submarines and air traffic control on carriers to microgrid power facilities and fuel depots on bases, many of the 16 critical infrastructure sectors are represented in defense systems and environments.



[2] *https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf*
[3] *http://themilitaryengineer.com/index.php/component/k2/item/261-cybersecuring-industrial-control-systems*

Unfortunately, while traditional network and IT security within the DoD has been exemplary, the security of these critical infrastructure systems has lagged. While the cyber risk to critical infrastructure represents only a fraction of the total risk landscape, due to the exponential increases in threats and the effectiveness of attacks, it is quickly becoming an area of focus both within the government and private sector.

> *"We need to shift because that's not the only thing the information network is. It's also our platform IT; it's also all of our programs of record; it's also our ICS and SCADA systems; it's also the cloud; it's also all of our crossdomains that we have out in the network."*
>
> **- Col. Paul Craft, Dir. of Operations Joint Force Headquarters - DoDIN**[4]

Unlike defense and government IT systems, and despite the dramatic rise of cyber threats facing them, critical infrastructure security efforts are largely voluntary and supported primarily by internal resources in both the government and private sector.[5]

Challenges

The lack of standardized regulation and available security tools has its roots in a number of inherent complications and challenges with critical infrastructure cybersecurity.

Awareness

Among the myriad challenges to protecting critical infrastructure, none may be so pervasive and problematic as the collective societal assumptions of its existence such that it becomes practically invisible. So important is its uninterrupted, ongoing operation that no one outside those directly involved in its operation seems to think much about the power plant until the day the power goes out, or clean water until the water sanitation plant breaks down. Today, however, the cyber threats to critical infrastructure are too prevalent and dangerous to ignore any longer and have forced both the private sector and government to address its security.

Prioritization

For years, critical infrastructure was traditionally disconnected or "air gapped" from external networks and the internet. This allowed organizations to focus on physical security, safety, and productivity/uptime while awareness and investment has remained generally poor regarding cybersecurity. This also included industry research, regulatory best practices, and vendor/OEM investment – the lack of specialized ICS/OT security tools and guidance available for asset owners to protect their equipment left even those who wanted to act inadequately armed to do so.

Indeed, only after the Ukrainian power grid was breached and taken down in 2015, in one of the world's most sophisticated cyberattacks,[6] did the Department of Homeland Security (DHS) release a cybersecurity action plan outlining concrete steps to protect industrial control systems.[7] The DoD has also typically focused on protecting classified networks and information first, rather than NIPR Net or unclassified systems. Cybersecurity awareness from the top of the command chain down is a vital (and often missing) first step in developing a critical infrastructure security policy.

[4] *https://www.fifthdomain.com/dod/cybercom/2018/05/23/are-dods-cyber-forces-too-focused-on-the-network*
[5] *https://www.dhs.gov/cisa/supporting-policy-and-doctrine*
[6] *https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf*
[7] *https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf*

IT / OT Security Paradigm Shift

Many assume that all that is required to protect critical infrastructure is to extend the existing IT cybersecurity tools and policy to those systems. Unfortunately, there are a number of significant differences between protecting traditional IT systems versus the OT systems present in many critical infrastructure environments. Traditional IT security tools are not designed for the operational technology and industrial controls inherent in critical infrastructure. Scanning tools may overwhelm ICS devices resulting in failure, connecting OT equipment to IT systems can unintentionally expose it to the internet,[8] and firewall rules may disrupt process flows unexpectedly. Beyond that, the technology itself has unique challenges in lifecycle, downtime, and patching.

ASPECT	IT	OT
Awareness	High in both Private Sector and Government	Low Regarding Cybersecurity
Technology Lifecycle	3-5 Years	10-20 years or Longer
Patching	Regular/Weekly	Rare if Ever, Scheduled Months in Advance
Availability	Downtime Acceptable with Advance Notice	Continuous Operation – Downtime Generally Only in an Outage
Compatibility	Common, Widely Used	Rare, Difficult to Integrate
Physical Security	Very Good, Commonly Integrated with RBAC Tools	Very Good, but Often Remote and Unmanned

In addition, while the growing connectivity (aka "convergence") between OT and IT systems introduced greater efficiencies, it failed to account for security. While the IT security systems had years of maturity behind them, OT security had gone nowhere. This left connections into exposed, vulnerable OT infrastructure from the business network and internet at large, and inevitably led to successful IT-to-OT malware attacks such as Stuxnet,[9] Shamoon,[10] and BlackEnergy.[11]

Fit for Purpose

For years, the ICS devices inherent in critical infrastructure – SCADA systems, PLCs, data historians, etc. – have been optimized for things like peak productivity, low energy use, and long lifespan, and security was often last on the list, or left off altogether. Changing one component within the device may involve changing many others to accommodate, which can be particularly problematic in the defense context, as it may make the equipment no longer fit in its prescribed space, draw too much power, or create too much heat. The entire device may need to be redesigned, and in some cases, the manufacturer or user may make the determination that it's simply not worth it to change.

Even when some security has been built-in, OT systems and devices are often set up to fail, with outdated operating systems, open firmware, and hard-coded passwords. There may even be no memory available for patching bugs or vulnerabilities. The unique protocols and data types may introduce other problems, not to mention the lack of security skills and resources required for the dedicated management and frequent policy and software updates inherent in many IT security tools.

[8] *https://www.shodan.io*
[9] *https://ics-cert.us-cert.gov/advisories/ICSA-10-272-01*
[10] *https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B*
[11] *https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01*

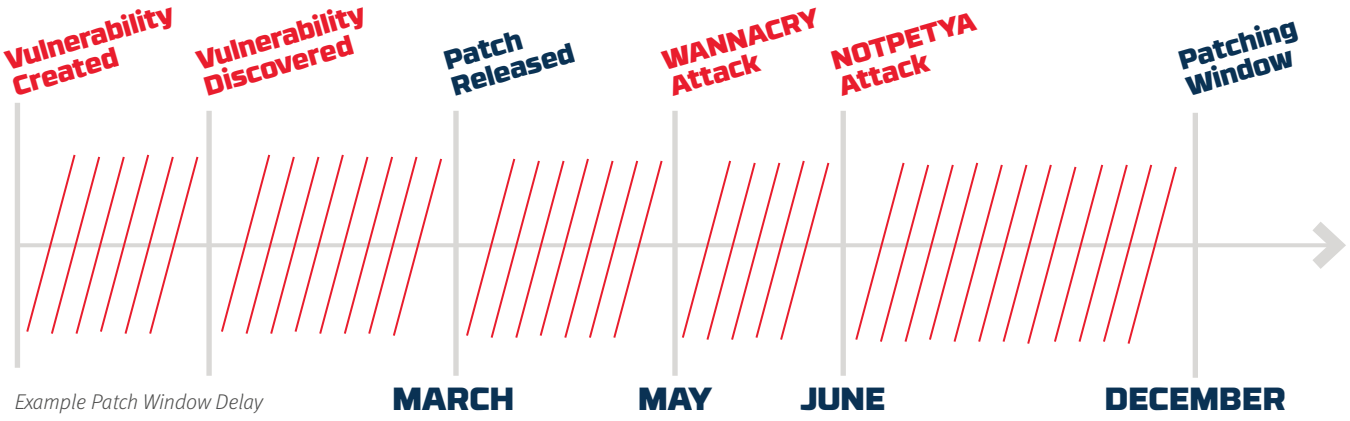
Lifecycle & Refresh

The lifecycle for critical infrastructure systems and devices may stretch on for decades – far longer than typical IT equipment lifecycles of 3-5 years. Since they've probably not been updated – or if add-on security is not possible – they'll need to be replaced to be secure. Also, replacement can and will cause significant (and unacceptable) disruption to day-to-day operations, so this virtually guarantees that unless the update is critical, systems will not be replaced until their lifecycle is up, which could be many years.

Due to the long lifespan of the equipment, sustainability tends to be far more important for security tools in critical infrastructure than in the IT space. Security solutions that can come close to or meet the expected equipment refresh lifecycle of 10 to 20 years can help avoid the disruption of change management, which is invaluable when downtime is nearly non-existent.

Patching

Keeping up to date on software patching is a cybersecurity best practice noted in virtually every source of guidance available. However, patching critical infrastructure systems can problematic for numerous reasons. First and foremost, any changes in critical infrastructure can require months of planning, as any downtime is far more significant than in the IT space. This typically requires waiting until the next "patch window" when a number of accumulated patches are all installed at once, in order to maximize the utility of the limited downtime. Unlike the "Patch Tuesday" world of IT where patches are regularly and often automatically applied, patch windows in critical infrastructure may only occur once or twice per year.



Example Patch Window Delay

OT systems are also typically combined from a set of diverse equipment manufacturers, each with their own vendor-specific patches. Gathering patches from multiple sources with various levels of support and staggered timing can be a time-consuming and arduous task. This is difficult enough in and of itself without considering that ICS patch programs may not be well established, the equipment is often older and easily outruns typical support lifetimes, or may not be designed with the free memory to update it at all.

In other cases, operators may run the risk/benefit analysis and choose not to patch. This is to ignore that many modern attacks can completely destroy entire critical infrastructure and OT networks,[12] and that it's not really a matter of if the network will get attacked, but when. Regardless, the most common reason given is simply because the systems work as is, and no one wants to perform change management, deal with any downtime, or risk disruptions and possible cascading failures.

[12] *https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet*

Downtime

Critical infrastructure by its very nature typically needs to be available all the time, 24x7x365. This is especially true in a DoD context where the systems may be operating in remote areas, e.g. shipboard systems out at sea, mobile communications towers active in the field, or power generators operating at a remote firebase. Not only are they vital for the continued day-to-day operations, but losing the support of critical systems may compromise mission success.

Third-Parties & Outsourcing

While adding in connectivity to native critical infrastructure technology can create security issues, incorporating connected third-party technology may only multiply security headaches. Additional update schedules, unknown or backend APIs, proprietary services, and configuration limitations are only a few of the potential issues from connected third-party technology. In some cases, the vendors themselves will require access to their equipment, opening yet another possible attack vector into the OT environment.

Generally, a significant amount of third-party risk can be avoided through a selective procurement process, but in many cases that process is driven by IT, rather than OT. With an entirely different set of priorities and a lack of process awareness, IT will often fail to consider some of the vital issues and effects on regulatory requirements that a particular technology could cause, creating a cascade of problems down the line.

Guidance and Best Practices

The Department of Defense Cyber Strategy (2018)[13] states "the Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability."

Due to the limited guidance currently available specifically for critical infrastructure in the DoD, an amalgam of associated best practices and regulations from various regulatory bodies and industry standards must be used to synthesize an interim framework. As a pre-existing federal standard, the Framework for Improving Critical Infrastructure Cybersecurity from NIST[14] serves as a useful outline to build such a working model for the DoD.

Separated into five distinct Functions, the Framework Core lays out the set of primary activities around which a comprehensive critical infrastructure security program can be designed, implemented, and refined. These five Functions are: Identify, Protect, Detect, Respond, and Recover.

NIST Cybersecurity Framework Core Structure

Identify

"Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities."

Much like the NIST 800-53 Risk Management Framework (RMF)[15] the "starting point" for any cybersecurity program is to identify organizational inputs, such as laws, directives, regulatory requirements, and guidance, as well as strategic goals and context to the greater organization, and specific technical requirements of the environment and the solution. As previously discussed, critical infrastructure lacks a structure of formalized regulatory requirements, therefore the strategic goals, best practice guidance, and technical requirements comprise the majority of this Function.

[13] *https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF*
[14] *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf*
[15] *NIST Special Publication 800-53 Rev 4, page 8*

Strategic Goals

According to the NIST Framework, "The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be."[16]

This assessment should begin with a thorough internal inventory or audit of connected systems, to identify potential threat vectors and define the risk level to various systems, devices, and networks/segments. This may or may not be equivalent to the assumed risk levels to the assets of the larger surrounding environment, such as an airbase, a ship, or an office building.

Many private sector and government organizations do not have accurate maps of data flows or system architectures for critical infrastructure environments, but they are vital for effective cybersecurity. Unless all of the possible points of vulnerability have been identified, there's no way to adequately prioritize risk or develop a meaningful strategy. An audit in critical infrastructure environments is typically performed manually. The reason for this is, as previously mentioned, the use of an automated network device mapping tool may potentially disrupt or overwhelm operational equipment by adding even a tiny extra load on the network.

Best Practices

Among the best practices outlined in the U.S. Department of Homeland Security's invaluable white paper, *Seven Steps to Effectively Defend Industrial Control Systems*,[17] perhaps the most important is to create a more easily defendable environment. First, by removing any unnecessary connections. This also includes connections to third parties that do not require access into the critical infrastructure/OT network.

Every connection to an external network, no matter how well monitored, is a potential avenue for attack into the critical infrastructure network. Many operators are stretched thin on cybersecurity to begin with – some don't even have a single dedicated role for it – so for each connection that is removed it is one less requiring protection, attention, and vigilance from a shorthanded group. Creating a defendable environment also means segmenting the critical infrastructure network itself, and creating layers of security within it, typically with a firewall, or in the case of critical infrastructure, a stronger security solution such as a data diode.

Technical Requirements

The operational technology and industrial control systems within critical infrastructure environments requires security solutions that are tailored or flexible enough to handle industrial protocols and interface with proprietary OEM equipment that are not typical in IT environments.

To develop a comprehensive set of technical requirements, the Interagency Security Committee (ISC) recommends that organizations and their CSOs "should coordinate with … stakeholders located at individual facilities, to establish a standing core team to address all aspects of mitigation measures under consideration." [18] Further, that CSOs "should include individuals from the IT community (when technology is being considered as a mitigation measure), [and] facility management (ensuring facility management is cognizant of risks identified and mitigating measures)."

[16] *NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, page 20*

[17] *https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%2Control%20Systems_S508C.pdf*

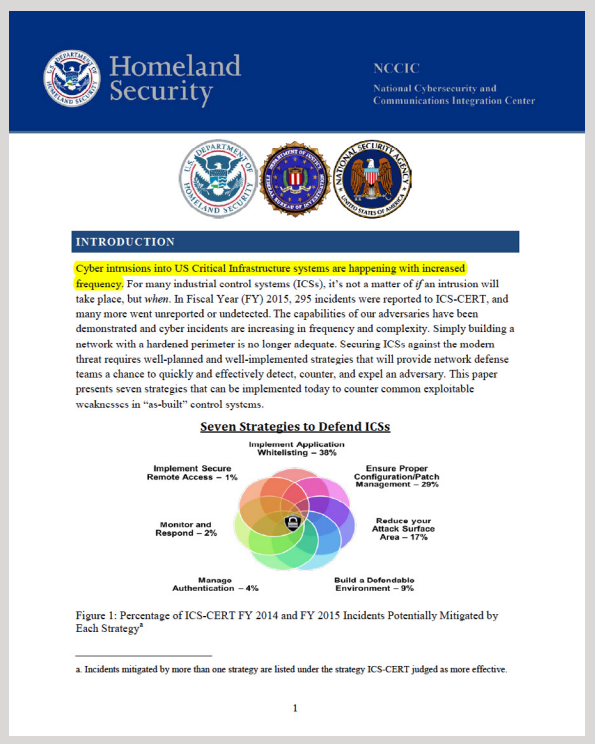
[18] *ISC - Securing Government Assets through Combined Traditional Security and Information Technology: An Interagency Security Committee White Paper, page 5*

Protect

"Develop and implement appropriate safeguards to ensure delivery of critical services."

One of the most concise and effective collections of guidance for protecting critical infrastructure and industrial control systems is the aforementioned white paper from the DHS and NCCIC titled, Seven Steps to Effectively Defend Industrial Control Systems. In fact, so effective are the steps outlined that according to the paper, "If system owners had implemented the strategies … 98 percent of incidents ICS-CERT responded to in FY 2014 and FY 2015 would have been prevented. The remaining 2 percent could have been identified with increased monitoring and a robust incident response." Six of these seven strategies fall under the Function of Protect, while the seventh is split under Detect and Respond:

- **APPLICATION WHITELISTING** - Only allows predesignated applications to run, no need to be aware of new threats as only authorized software will run.
- **CONFIGURATION & PATCH MANAGEMENT** - Adversaries will always target a weak point or vulnerability. A system that is not hardened or is out of date becomes a target. Ensure systems are up to date, that external connections to the control network are limited and a secure method for introducing authenticated software patches is used.
- **REDUCE ATTACK SURFACE AREA** - Isolate industrial control system (ICS) networks from untrusted networks, lock down unused services and ports, use a data diode to provide network segmentation, and if bidirectional communication is needed, use a single port over a restricted path.
- **BUILD A DEFENDABLE ENVIRONMENT** - Limit damage from network perimeter breaches. Segment networks and restrict host-to-host paths to prevent and contain the spread of infection.
- **MANAGE AUTHENTICATION** - Prevent adversaries from masquerading as legitimate users. Stress length of passwords over complexity, reduce privileges to only those needed for each user class, change passwords at least every 90 days, require separate credentials for corporate (IT) and control network (OT) zones.



Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

INTRODUCTION

Cyber intrusions into US Critical Infrastructure systems are happening with increased frequency. For many industrial control systems (ICSs), it's not a matter of *if* an intrusion will take place, but *when*. In Fiscal Year (FY) 2015, 295 incidents were reported to ICS-CERT, and many more went unreported or undetected. The capabilities of our adversaries have been demonstrated and cyber incidents are increasing in frequency and complexity. Simply building a network with a hardened perimeter is no longer adequate. Securing ICSs against the modern threat requires well-planned and well-implemented strategies that will provide network defense teams a chance to quickly and effectively detect, counter, and expel an adversary. This paper presents seven strategies that can be implemented today to counter common exploitable weaknesses in "as-built" control systems.

Seven Strategies to Defend ICSs

Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[a]

a. Incidents mitigated by more than one strategy are listed under the strategy ICS-CERT judged as more effective.

1

- **IMPLEMENT SECURE REMOTE ACCESS** - Remove back doors and modem access, implement monitoring-only access, enforced by data diodes, do not rely on "read only" software configurations, and do not allow persistent remote connections.
- **MONITOR & RESPOND** - More on this in the next two sections, but the DHS recommends that organizations watch traffic on ICS boundaries, monitor traffic within ICS network, use products to detect malicious software and attacks, perform login analysis, watch for access control manipulation.

Technology

In order to accomplish the seven steps, the DHS also recommends the use of various technologies and techniques, including application whitelisting, mutli-factor authentication, and "optical separation" with a data diode. Software security solutions like firewalls are ubiquitous in IT. However, they are not designed for OT systems, and even the specialized "industrial" firewalls that are essentially simplified versions of the IT-based device often fail to provide adequate levels of security to high-risk assets in critical infrastructure. Hardware-enforced solutions, such as data diodes, are far better aligned to OT technology, with far longer lifespans, minimal maintenance requirements, and interfaces designed for ICS equipment. The enforcement mechanism within data diodes is also far stronger than software-based tools. The optical separation is based on the laws of physics, rather than malleable policy configuration, which makes them essentially unhackable by virtual or electronic means. Data diodes are also commonly used in the DoD within cross domain solutions, with added specialized filtering and data validation software.

Detect

"Develop and implement appropriate activities to identify the occurrence of a cybersecurity event."

Network monitoring tools such as Sophia [19] have been in use across the DoD for years, and can be utilized in critical infrastructure to help baseline "normal" or expected behaviors on OT networks. There are now many ICS monitoring tools available to critical infrastructure operators, although the utility of detecting attacks may be limited as attackers may have already gained access into the network. In some cases this may mean a malicious insider, which is one of the most difficult threats to address. Ideally the defense-in-depth architecture and "least privilege" principles from the cybersecurity policy should help to detect these issues by limiting the access to sensitive systems and devices. Once any attempt outside these bounds is made, the system will more easily be able to detect the anomaly.

Respond

"Develop and implement appropriate activities to take action regarding a detected cybersecurity incident."

The DHS recommends that critical infrastructure operators "have a response plan for when adversarial activity is detected." Response plans in these environments vary in scope and may have substantial safety elements based on the dangers presented by the equipment present (nuclear reactors, dams, etc.). "Such a plan may include disconnecting all Internet connections, running a properly scoped search for malware, disabling affected user accounts, isolating suspect systems, and an immediate 100 percent password reset." There may be other regulated activities such as escalation, outside agency incident response, and investigation, as well as possible public affairs activities.

Recover

"Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident."

Again, the DHS recommends that operators "have a restoration plan, including having "gold disks" ready to restore systems to known good states." In the case of critical infrastructure, there may be devices and systems that have no backup state. Some of the more recent automated processes may actually lack a manual override. In these cases, the DHS recommends replacing these devices, otherwise operators may not have any recourse but to permanently shut down or destroy the devices in case of cyberattack. In addition, operators should utilize the knowledge gleaned in their response and recovery process in order to revise and strengthen their cybersecurity strategy and policy.

In order to help critical infrastructure operators within the DoD to improve their cybersecurity posture, the National Cybersecurity and Communications Integration Center (NCCIC) provides cybersecurity assessments of critical infrastructure within the Federal Government. These "Industrial Control Systems Federal Critical Infrastructure Assessments" (ICS-FCIA) are comprehensive cybersecurity evaluations focused on the defense of critical control systems against advanced persistent threats.

Summary

While regulations are limited, critical infrastructure operators within the DoD are well served to bring the appropriate focus to the cyber defenses of their systems and devices. The effects of a possible cyber attack are potentially catastrophic, and the chances of such an attack are only growing every day. Therefore prioritizing and implementing a comprehensive cybersecurity program should be of paramount importance. Unless such a program is brought to the fore and properly funded, the DoD (and the private sector) risk operational readiness and perhaps significant loss of life. Thankfully, there are plenty of new tools and technologies specially designed to secure the operational systems, and by following closely the lessons learned and best practices available, operators can help to protect the critical assets of the DoD and United States of America.

[19] *https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493842483.pdf*

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com