HANDBOOK

for

SELF-ASSESSING SECURITY VULNERABILITIES & RISKS

of

INDUSTRIAL CONTROL SYSTEMS

on

DOD INSTALLATIONS

19 December 2012

This handbook is a result of a collaborative effort between the "Joint Threat Assessment and Negation for Installation Infrastructure Control Systems" (JTANIICS) Quick Reaction Test (QRT) and the Joint Test and Evaluation (JT&E) Program under the Director, Operational Test and Evaluation, Office of the Secretary of Defense. The JT&E Program seeks nominations from Services, combatant commands, and national agencies for projects that develop test products to resolve joint operational problems. The objective of the JT&E Program is to find ways for warfighters to improve mission performance with current equipment, organizations, and doctrine.

Please visit www.jte.osd.mil for additional information on the JT&E Program.

Handbook content is a result of the combined work of the 346th Test Squadron, 262d Network Warfare Squadron, and the Idaho National Laboratory under the aegis of the Air Force Joint Test Program Office with advice of Joint Warfighter Advisory Group (JWAG) members/stakeholders. Myriad of other agencies influenced content by means of their publications (sources listed in an appendix).

Contents

Figures

With mission assurance utmost in mind, this handbook is intended to provide an installation commander & staff with a generalized approach to eliminate, minimize, or otherwise mitigate risks to the mission as posed by Industrial Control System (ICS) vulnerabilities.

"The most common cause of task degradation or mission failure is human error, specifically the inability to consistently manage risk."

OPNAVINST 3500.39C (2010), para. 4

Industrial Control Systems

Vulnerability & Risk Self-Assessment Aid

EXECUTIVE SUMMARY

Key Points

- The primary goal is mission assurance.
- The primary focus is on risk management.
- The primary audience is the installation commander, with his or her staff as close secondary.
- The primary intent is to facilitate self-assessment of Industrial Control Systems (ICS) security posture vis-à-vis missions' priorities.
- The primary approach is generic, enabling broad (Joint/all Services) utility.

One of the essential responsibilities of the installation commander and supporting staff is to manage risks to establish optimal conditions for assuring successful accomplishment of assigned missions every day. Although not always obvious, many missions depend on the unfailing functioning of ICS and therefore on the security of those systems.

A mission assured today is never taken for granted as assured tomorrow. Mission assurance demands constant vigilance along with proactive risk management. Risks come in myriad shapes and sizes—some enduring, some sporadic and situational, others appearing without warning. ICS represent only one set among a vast array of mission vulnerabilities and risks, an array that often competes for resources and, therefore, requires prioritization of management actions.

This handbook is intended for use primarily by Department of Defense (DOD) installation commanders, supported by staff members, as a **management tool** to self-assess,[1] prioritize, and manage mission-related vulnerabilities and risks that may be exposed or created by connectivity to ICS. ICS include a variety of systems or mechanisms used to monitor and/or operate critical infrastructure elements, such as electricity, water, natural gas, fuels, entry and access (doors, buildings, gates), heating & air-conditioning, runway lighting, etc. Other terms

[1] Other entities and programs are available to conduct formal and very thorough technical assessments, but those must be coordinated, scheduled, and resourced (i.e., funded). This aid provides an ability to conduct self-assessments when/as necessary or desired, and thereby, also the ability to prioritize and manage the resources required to address identified vulnerabilities and risks.

often heard include SCADA, DCS, or EMCS.[2] Throughout this book the term "ICS" is used as encompassing such variations.

This book is intentionally generic. Whatever the category of ICS, the *approach* to vulnerability assessment and risk management is similar. The applicability of actions recommended here may be extended to any DOD military installation regardless of the specific categories of ICS encountered. In keeping with the generic approach and due primarily to the unique nature of each installation's infrastructure, beyond a couple of exceptions there are no checklists, standard operating procedures (SOP), or similar sets of lock-step actions provided here. However, a risk management team using the handbook likely will want to develop checklists tailored to their specific circumstances.

Among other purposes, this handbook is intended to increase awareness of how a threat related to the ICS itself translates into a threat to the mission, either directly through the ICS or circuitously via network connections. Every military installation has numerous mission-support processes and systems controlled by, or that otherwise depend on, ICS. Every connection or access point represents potential vulnerabilities and, therefore, risks to the system under control (i.e., electrical, water, emergency services, etc.), which can escalate quickly to adverse impact on mission essential functions (MEF) and mission accomplishment.

Fundamentally then, this handbook is provided to help the installation leadership conduct a risk self-assessment focused on ICS and supported missions and then implement plans to manage that risk. Most of the information contained herein is not unique to this publication. Two unique aspects are: (1) the aggregation of disparate information into one place, distilling essentials, and tailoring to DOD installation leadership; and (2) bringing cyber/information technology (IT), civil engineers, public works, and mission operators together with a singular focus on ICS security in support of missions. This handbook (via Appendices) also points to additional resources.

The key set of activities—one exception to the "no checklists" approach—is found under the heading "**ICS Security Assessment Process**." Succinctly the process consists of eight steps, which if implemented with deliberation and in a team environment, will set the success conditions for all other actions recommended or suggested within this handbook (see Figure 1). This set of eight steps represents the core of the handbook. **All other information herein is intended to support implementation of those eight steps**.

[2] SCADA= Supervisory Control and Data Acquisition; DCS = Distributed Control System; EMCS = Energy Management Control System. Other variations exist; for example, building control systems.

Before explaining the eight-step assessment process, the handbook provides introductory, informative and supporting information. Closely aligned with and serving as companion to the "Assessment Process" is a section titled "**Framework for Successful ICS Defense**." If the installation does not already have a single ICS manager and/or team, the "Framework" should be considered prior to engaging on the eight-step process.

Figure 1. ICS Security Assessment Eight-Step Process

INDUSTRIAL CONTROL SYSTEMS "101"

Key Point

- Understanding ICS is not difficult; the challenge is to understand the ICS relationship to missions.

Fundamentally Industrial Control Systems (ICS) are systems and mechanisms that control flow. ICS control flow of electricity, fluids, gases, air, traffic, and even people. They are the computer-controlled electro-mechanical systems that ensure installation infrastructure services are delivered when and where required to accomplish the mission. In the electric infrastructure, they control actions such as opening and closing switches; for water, they open and close valves; for buildings, they control access to various doors as well as operation of the heating, ventilation, and air conditioning (HVAC) system.

The term "Industrial Control System" is broad; specific instances of ICS may be called Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Energy Management Control System (EMCS), Emergency Medical Service (EMS), or other terms but all perform the same fundamental function. Also, on DOD installations, ICS are associated primarily with infrastructure elements; therefore, though not technically accurate, they may be referred to as "Infrastructure" vice "Industrial" control systems. The hardware components that comprise an ICS usually are classed as operational technology (OT) versus information technology (IT), which refers to (among other things) the computer equipment that sits on nearly every desk. Another term used in this domain is Platform Information Technology (PIT),[3] (and PITI, with the 'I' referring to interconnect, or connected to the network) although ICS are only one sub-category of PIT, which also includes weapons systems, aircraft, vehicles, buildings, etc. Terminology is not that critical. What is important is to know that ICS are critical to the mission.

You frequently have used an ICS—though not by that term—in your home. It is called a "thermostat." The most simple of thermostats may not be so obvious as an ICS, but the more sophisticated can be programmed to automatically control the flow of air (heated, cooled, or just fan) by day, time, room, zone, etc. The most advanced allow the owner to monitor and operate the system over an Internet connection or Wi-Fi, using a Smartphone or tablet.

The "Smart Grid," once fully implemented, will allow your utility company to operate your thermostat remotely. The thermostat monitors temperatures (and some include humidity) and

[3] "PIT" is used more by the Air Force and to a lesser extent by the Navy. At the DoD level, PIT is addressed mostly under information assurance (IA) guidance, such as DODI 8500.2. See the Glossary for a DOD definition of PIT.

then operates the electro-mechanical equipment (furnace, air conditioner, fan) to respond to the preset conditions you have selected. If the thermostat fails—even though the mechanicals are in perfect operating condition—the mission (cool, heat) fails. This same concept translates to the installation's missions: if the ICS fails the mission can fail, although the direct cause and effect may not always be so obvious.

ICS typically are not visible to the general population. The control devices themselves are behind panels, behind walls, inside cabinets, under floors, under roads; the master control computers more often reside in a room in a civil engineer (CE) or public works (PW) facility. Because they are essentially invisible to all but CE and PW, and are considered as simply infrastructure elements, ICS often are overlooked when assessing mission dependencies. Regardless of where they physically reside or who directly operates the ICS, every person and every mission on the installation is a stakeholder in their properly functioning.

While the ICS field (vs. control room) elements consist of mostly electro-mechanical devices, some are actually computers that control other field devices and communicate with other computers in the system with minimal human interaction. The most common example of this type is the Programmable Logic Controller (PLC).[4] PLCs (and their cousins, Remote Terminal Units or RTU) are very important because they are computers, typically not under direct human supervision, and offer multiple pathways (e.g., wireless, modem, Ethernet, Universal Serial Bus [USB]) for connecting to both the controlled infrastructure and the network. This combination of characteristics makes the PLC an especially vulnerable node in the ICS.

At the front end—the control center—is where most of the computers (servers, system interfaces, etc.) and, more critically, **connection** to other networks reside. While PLCs/RTUs may become connected (autonomously or by human intervention) for intermittent periods, control center computers may be continuously connected[5] to the Non-secure Internet Protocol Router Network (NIPRNet), other elements of the Global Information Grid (GIG), and/or an Internet Service Provider (ISP). It is especially at this node that ICS should be treated with the same security considerations as with IT.
Whether an ICS element is continuously or only intermittently connected presents the same fundamental security issue. Anytime an element is connected to a network, even if for only

[4] Many will recall that a Siemens PLC was the primary target for the Stuxnet code that impacted the centrifuges in the Iranian nuclear processing facility at Natanz in 2010. This same PLC (or variants) can be found in the critical infrastructures on numerous DOD installations. See an informative Wikipedia article on Stuxnet here: http://en.wikipedia.org/wiki/Stuxnet

[5] Another term used here is PIT-I, or PIT-Interconnect—that juncture where the ICS (or OT) connects with the IT network. For detail on PIT and PIT-I, in addition to DODI 8500.2, see: DODD 8500.01E; AFI 33-210 with AFGM2.2; AFCESA ETL 11-1; DON CIO Memo 02-10 and Enclosures.

brief instances, it is vulnerable to destructive attack, compromise, or manipulation. Therefore, when assessing risk the **key question** is not "Is it connected?" but "Is it connect-able?" Network mapping (via software) will not reveal such potential connectivity; only a physical, visual inspection of an element by a knowledgeable expert (more likely an IT than a CE or PW person) will yield specific information on what type of connection ports exist on what elements. Where the location of an element makes visual inspection impractical or impossible, use the manufacturer's or vendor's published manuals for that specific piece of equipment.

Understanding the fundamentals of ICS is not difficult. The challenge is in understanding the dependencies of mission on ICS and therefore, appropriately managing the risks to the ICS and to the missions they support. This handbook is intended to assist the commander and staff in gaining that understanding.

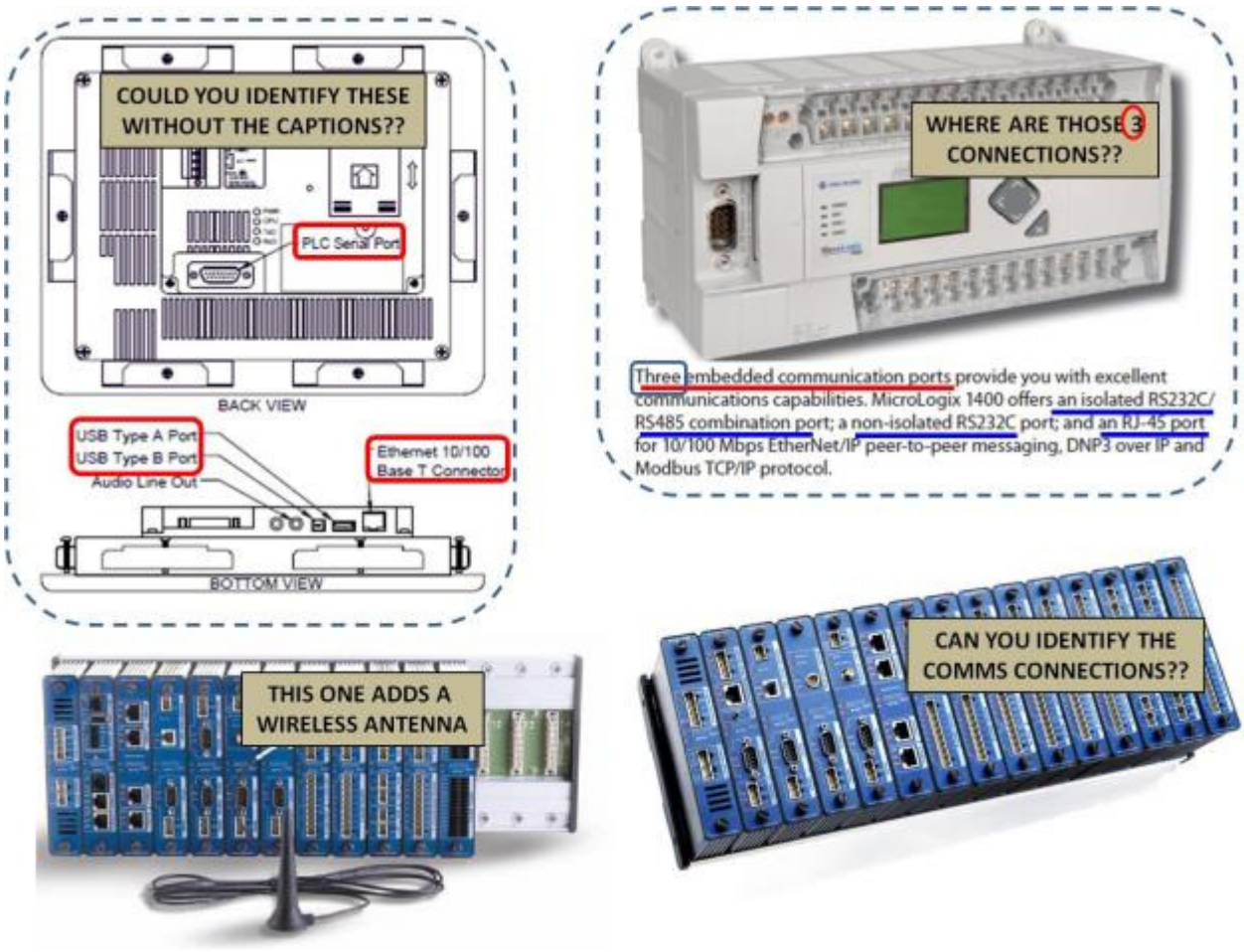


Figure 2. PLCs & RTUs: The Challenge of Finding the Connectivity

HANDBOOK AUTHORITIES

Key Point:

- The handbook reflects breadth and depth of ICS community expertise.

This handbook was developed based on a broad collection of authoritative sources;[6] underwent field testing to validate the framework and applicability at the installation command level; was reviewed by a Joint Warfighter Advisory Group (JWAG[7]) to verify broad (i.e., Joint) applicability; and received direct input by a broad-based selection of ICS and risk management subject matter experts (SME). Users of this handbook will gain even greater value by referencing current publications of primary sources. Some of the major publications are listed in Appendix A, References. Note that while this handbook is advisory, many of the sources are authoritative and/or directive.

DISTINCTIONS BETWEEN ICS AND IT

Key Point:

- ICS and IT share similarities, but also have unique characteristics.

Fundamentally ICS security is a combination of IA, cyber security, physical security, and operations security (OPSEC). This same combination is applicable to IT, so is there any difference between ICS and IT? Yes. One key distinction between ICS and other IT architectures is that the physical world can be impacted disastrously by malicious (or only accidental) manipulation of the ICS. For example, with IT there typically is linkage with only other IT components; with ICS the linkage can be to the electric grid, powering other critical assets, as well as to other infrastructure elements. This gives rise to another primary distinction, namely that ICS must always be available while "pure" IT can survive downtimes. Another important difference is in the "refresh" rates of the technologies: IT tends to turn over in three years or less while OT (ICS) can be on a 20-year cycle. Why is this important to know?

---

[6] Among sources: Idaho National Laboratory (INL); AF Civil Engineer Support Agency (AFCESA); Department of Homeland Security DHS ICS-Computer Emergency Response Team (CERT); the National SCADA Test Bed (NSTB); DHS Center for the Protection of National Infrastructure (CPNI); National Institute of Standards and Technology (NIST); National Security Agency's (NSA) Committee on National Security Systems (CNSS); Federal Information Processing Standards (FIPS); and numerous SMEs who are members of or closely associated with the DoD.

[7] JWAG participants may differ from meeting-to-meeting, but broadly represent stakeholders in the outcome or product of a specified Joint activity or project. For this handbook the initial JWAG included representatives from United States Cyber Command (USCYBERCOM), Northern Command (NORTHCOM), AFCESA, INL, Sandia National Laboratory (SNL), and various CE and communications experts from both Army and Air Force elements of Joint Base San Antonio.

The long refresh cycle of ICS results in hardware, software, and operating systems no longer supported by vendors. The impacts of lack of support include: woefully stale malware detection programs, operating systems that cannot handle newer (and more efficient/effective) software programs, and hardware that may be on the verge of catastrophic failure with no backup or failover equipment available.

The following extract from NIST Special Publication 800-82[8] provides an excellent review of not only the distinctions but also the similarities and how OT (such as ICS) and IT are converging.

> "Initially, ICS had little resemblance to traditional information technology (IT) systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As ICS are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.
>
> "Although some characteristics are similar, ICS also have characteristics that differ from traditional information processing systems. Many of these differences stem from the fact that logic executing in ICS has a direct affect on the physical world. Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation's economy, and compromise of proprietary information. ICS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems.

[8] NIST SP 800-82, 2011 version, Executive Summary, p.1.

> Originally, ICS implementations were susceptible primarily to local threats because many of their components were in physically secured areas and the components were not connected to IT networks or systems. However, the trend toward integrating ICS systems with IT networks provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats. Also, the increasing use of wireless networking places ICS implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, natural disasters as well as malicious or accidental actions by insiders. ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order."

Distinctions between ICS and IT aside, from a purely technical security standpoint, ICS may be considered on par with IT or IA vis-à-vis security challenges, albeit with warnings about use of certain software tools on the networks.[9]

THREATS

Key Point:

- Threats are global but assessments must be local.

What threats could be posed to an installation's mission by or through the ICS? This is an essential question, but one that cannot be answered specifically in an unclassified venue or simplistically in any venue. Generically, threats fall into categories similar to IT and/or cyber: terrorist, criminal, insider, environmental, etc. Use of this self-assessment handbook can lead to a deeper understanding of the infrastructure and establish mitigation conditions whereby specific threats may be identified. But even without specific threats known many risks can be

[9] Caveat emptor with respect to software tools. Software applications that test, penetrate, scan, characterize, and/or defend networks should be considered equivalent to "loaded weapons" with respect to control systems. Some tools that are entirely "safe" when used on IT networks have been demonstrated both in the field and under controlled conditions to have negative, even catastrophic effects on ICS networks. If such tools are considered for use on ICS, the decision must be an informed one and the tool operator must be a SME who understands potential effects of that tool on an ICS. Furthermore, any such use must be coordinated with the relevant IT agency (e.g., Service CERT) because tool use on the connected ICS could trip various IT network defense mechanisms (firewalls, intrusion detection system (IDS), intrusion prevention system (IPS), etc).

identified and managed. In other words, this handbook can help to establish a more effective and efficient security posture to conduct formal threat assessments.

The Security Incidents Organization in a 2009 survey (not specific to DOD) assessed that roughly 75% of ICS incidents were unintentional. Of the 25% that were intentional, over half were by insiders. In other words, external threat actors were responsible for events only about 10% of the time. Based on percentages alone, the hostile threat actor would *appear* to be of far less concern than a mistake committed by a legitimate operator. However, the external threat actor represents a potentially far more malicious and far-reaching impact on mission than either the intentional insider or unintentional event. Among external threats, perhaps the most insidious is the so-called Advanced Persistent Threat, or APT. The National Institute of Standards and Technology (NIST) (*et al*) assesses that the external threat actor found ways not only to get "inside" but also to stay there as long as he wants or needs. The APT,[10] especially nation-state sponsored, is perhaps the most ominous threat to DOD networks. Open source information on threats is plentiful and readily available, but ICS security teams will need access to classified intelligence resources to obtain more "actionable" information.

> "The increasing interconnectivity and interdependence among commercial and defense infrastructures demand that DOD take steps to understand and remedy or mitigate the vulnerabilities of, and threats to, the critical infrastructures on which it depends for mission accomplishment."
>
> *Joint Pub 3-27 (p. VII-8)*

MISSION PRIORITIES

Key Points:

- Missions are interconnected and mutually dependent in complex ways.
- Priorities tend to be situational and event-driven.

The US Navy, articulating what is essentially true for all the Services and including ICS as part of their cyber infrastructure, has stated:[11]

> "The Department of the Navy (DON) relies on a network of physical and cyber infrastructure so critical that its degradation, exploitation, or destruction could have a debilitating effect on the DON's ability to project, support, and sustain its forces and operations worldwide. This critical infrastructure includes DON and non-DON domestic and foreign

[10] NIST addressed the APT in Revision 4 to SP 800-53.
[11] *Critical Infrastructure Protection Program, Strategy for 2009 and Beyond*, 2009

infrastructures essential to planning, mobilizing, deploying, executing, and sustaining U.S. military operations on a global basis. Mission Assurance is a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is made more difficult due to increased interconnectivity and interdependency of systems and networks. DON critical infrastructures, both physical and cyber, even if degraded, must be available to meet the requirements of multiple, dynamic, and divergent missions."

> "Major ship systems may be impacted by SCADA network attacks ashore and afloat. This may impact a ship's ability to start or stop engines remotely disabling portions of the propulsion system and other engineering systems."
>
> *Navy TACMEMO NWDC 3-56.1-12*

Which ICS receive greater focus for security efforts will depend in most cases on what missions they support. The 262d Network Warfare Squadron (262 NWS) defines this as the "criticality" of the system component whereby lesser systems may receive little to no focus while very critical and centralized systems are recommended to be hardened and protected significantly. An example might be where it is impossible to protect every component on a network; focus would be on critical servers, in essence accepting the risk of an individual personal computer compromise so long as it can be isolated and secure operation of the critical server maintained.

But even on a given installation mission priorities—and the importance of the supporting control systems—can change quickly and without advance notice. Consider the following hypothetical scenario highlighting such a rapid change.

Daedalus Air Force Base's primary mission is undergraduate pilot training. Flight operations are essential to this training. Flight operations depend on, among other things, a well-managed fuels system and properly functioning airfield lighting—both systems controlled by ICS. Therefore securing the lighting and fuels ICS networks will be a priority over, for example, automobile traffic control systems elsewhere on the installation. At 1430 on Thursday, a terrorist incident results in declaration of Force Protection Condition (FPCON) DELTA. At 1431 the primary mission of the installation dramatically shifts from UPT to defense (of people, infrastructure, and physical assets). ICS that are essential now include vehicular traffic control (not so critical under FPCON ALPHA) and emergency services (including camera systems, alarms, door controls, EMS

> and fire department dispatch, etc.). As a result of the incident, one of the ICS was damaged. The ICS maintainer is a commercial contractor whose facilities are not on the base. The contractor has backups of the ICS operating system, programs and data, but all are at the contractor facility off base. Because of the elevated FPCON, the contractor cannot enter the base. CE can provide some limited manual operation of the system, but is neither capable nor prepared to operate at even 50% efficiency and effectiveness.

Is the installation prepared for departures from the norm where ICS are part of the equation? Do the various existing installation plans (incident response, disaster recovery, installation emergency management, etc.) encompass ICS contingencies and emergencies? If so, have such contingencies been exercised (not simply "white-carded" during an exercise)? These are some of the considerations that will prove foundational to identifying ICS security priorities relative to missions and changing mission priorities.

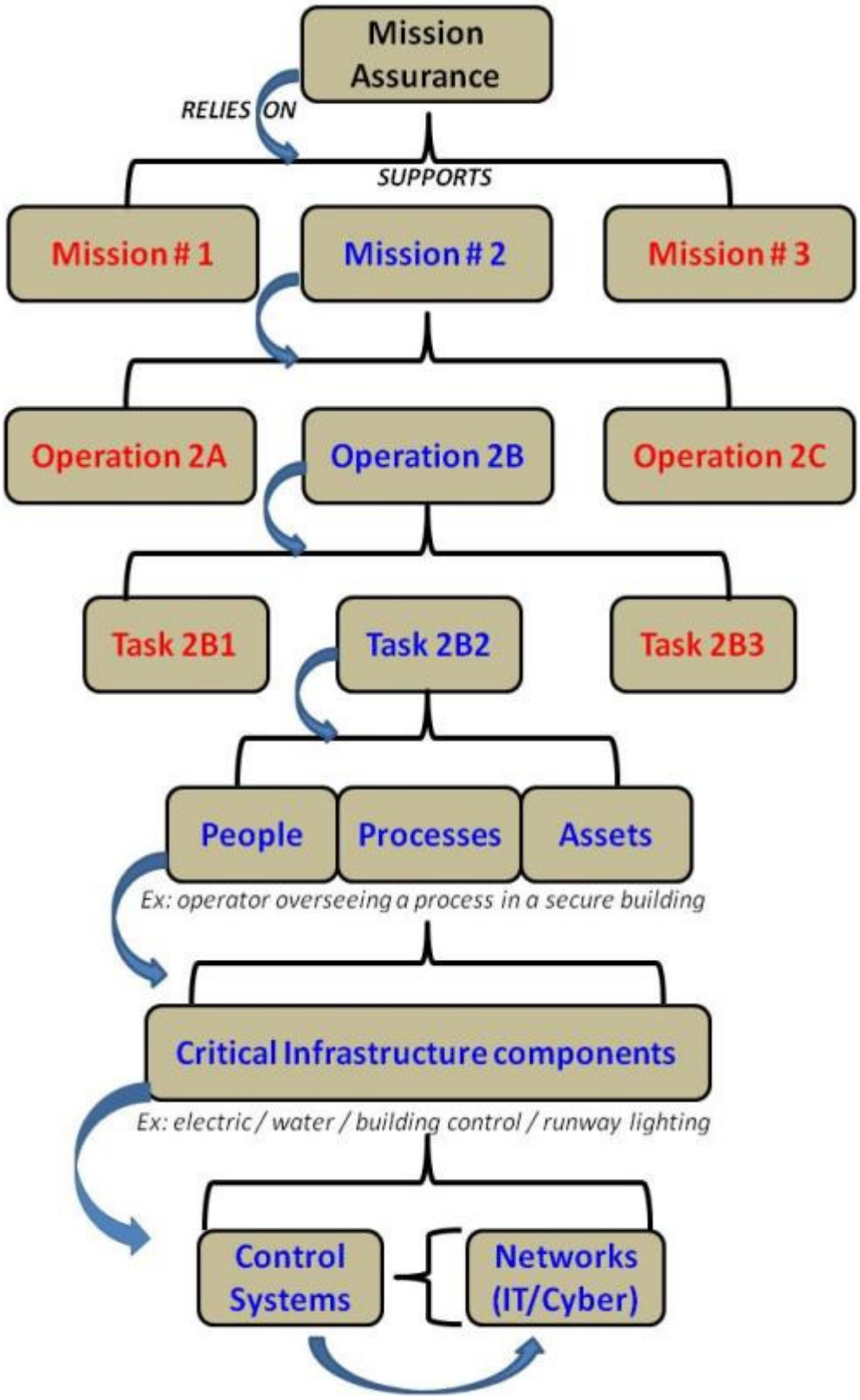


Figure 3. Mapping Mission Assurance to ICS

MISSION IMPACT

Key Point:

- If an element of the ICS and/or controlled infrastructure is compromised, critical mission functions may be degraded or even entirely failed.

For any installation commander, mission assurance is of utmost concern. Anything that may impact the mission rises to the top of the priority list. ICS and the controlled critical infrastructure are deemed to be mission enablers; damage to or compromise of ICS can degrade, compromise, or even deny the mission. With mission assurance foremost in mind, this handbook provides the installation commander with a generalized approach to eliminate, minimize, or otherwise mitigate risks to the mission as posed by ICS vulnerabilities.

It is important to note that this handbook does not attempt to achieve a level of specificity that addresses vulnerabilities of specific products from specific vendors in specific applications. Nor does it capture the range of threat actors who may be seeking to exploit those vulnerabilities. Such level of specificity must be addressed on a case-by-case basis under the collaborative efforts of the installation commander, CEs or PWs, communications element, and mission operations representatives, and, in some cases, external experts. Specifically for the threat piece of the equation, intelligence and/or law enforcement entities also must be consulted.

It is vitally important to understand that some mission-impacting vulnerabilities can be created at nodes where it may not be intuitively obvious. For example, consider a fuels control system directly supporting an operational mission. If this mission is assessed as high-priority, then the fuels control system (i.e., ICS) merits a commensurately high priority for defensive measures and may in fact be well defended. However there may be interconnections from non-mission-related systems linked back into those that are critical, opening paths of access to even defended nodes. For instance, there may be an unclassified IT network connection to the vehicle traffic control system, which in turn has a connection to the EMS management system, which in turn has a connection into the fuels management system. To discover which control systems may present vulnerabilities to the mission requires following the trail (virtually, logically, and physically) of all nodes and elements and their potential connections[12] as well as actual ones.

The probability of a threat actor finding and traversing all such interconnections to create negative effects on the mission may not be high at a given moment, but threat actors

[12] "Connection" includes wired network, wireless, radio, modem, USB port, Ethernet port….anything that enables one element to connect to another.

continuously develop more advanced skills.[13] Though current probability of a successful attack may not be high, the advanced skill sets available to malicious actors combined with more freely available advanced exploitation tools, many of which are created with ICS attack components or even specifically for ICS, make this a serious threat. No system or sub-system can be overlooked or assumed secure simply because it appears isolated. It is important to also note that a vulnerability and risk assessment should consider not just primary effects on a system, but potential second—and even third—order effects. Succinctly stated, an ICS vulnerability and risk assessment should be supported by a thorough mission effects assessment.

Prioritization of defense measures and resource allocation requires more than a one-to-one matching with missions, but rather needs to be approached comprehensively. There is added complexity created by Joint Base administration where one Service's primary mission likely is not the same as that of the other Services. Take for example a fuel delivery control system on a Joint Base hosting both Air Force and Army missions. For efficiency and cost savings, the fuels delivery systems and automated control may be consolidated. Hypothetically, for this installation the Air Force's primary mission may be to launch sorties providing defense of the North American airspace while the Army's may be to train vehicle maintenance and repair. If the Army is lead agent for the Joint Base, do they consider the fuels system as the top priority ICS to protect? How will this be decided where three or all Services are included in a Joint Base structure? Such questions underscore the imperative for a comprehensive approach.

> "The purpose of the Air Force's Critical Infrastructure Program (CIP) is to ensure Air Force's ability to execute missions and capabilities that are essential to planning, mobilizing, deploying, executing, and sustaining military operations on a global basis."
>
> *Air Force Energy Plan 2010 (p. 19)*

THE MOST SECURE ICS

Key Points:

- No ICS is 100% secure 100% of the time.
- Misconceptions → undetected or neglected vulnerabilities → unmanaged risk.

[13] For example, the ICS-CERT in Alert 12-046-01, February 2012, stated: "ICS-CERT is monitoring and responding to an increase in a combination of threat elements that increase the risk of control system attacks. These elements include Internet accessible configurations, vulnerability and exploit tool releases for ICS devices, and increased interest and activity by hacktivist groups and others."

An absolutely 100% vulnerability-free, risk-free ICS does not exist and likely will not. To be *nearly* invulnerable,[14] an ICS must not be connected to anything other than its own infrastructure elements. There also must be no potential method for external connections: USB ports, Ethernet ports, wireless access points, satellite radio, modems, etc. Additionally, there would have to be unassailable physical controls. However, vendors often need real-time access to the infrastructure, and operators cannot be in all places all the time, which typically is mitigated by remote access capability. Also, the ICS manufacturing industry favors connectivity especially for vendor maintenance. Further complicating the security task is DOD's "green" mandate to convert the electric infrastructure to the "Smart Grid," which depends on wireless connectivity.[15]

The following "Top ICS Security Misconceptions" were presented in "318 OSS/IN SCADA Threat Assessment Report".[16] Note that this list reflects ideas at a point in time and then only the top five are presented; there are other relevant misconceptions, and all will most certainly change over time. The point is simply that there is widespread misunderstanding about ICS security and that such misunderstanding can result in a less-than-secure system. For brevity, the "misconceptions" have been edited but retain the essential message of each as presented in the original report:

- Misconception 1: **ICS & SCADA Systems Have a Secure Software Profile**.

Discussion: Systems that manage the delivery of critical resources should be viewed as one of the nation's top security priorities. ICS has not yet achieved the same level of security concern as other cyber or IT resources. ICS typically are installed with *availability* as the primary driver and then operating efficiency and cost-effectiveness as secondary imperatives; robust security typically is an after-thought and sometimes not considered at all.

- Misconception 2: **ICS & SCADA Systems are Monitored by IT Professionals**.

Discussion: To those not directly involved it may seem that ICS falls under purview of the IT experts, but that typically is not the case. Most often CEs or PWs are responsible for not only the hardware elements of the infrastructure, but also the software and communications

[14] Complete invulnerability is unachievable especially where the human element is necessary—thus the insider threat is always a potential.

[15] For example, "demand-response" management by the EMCS connecting to any load (fuels, lighting, HVAC, whatever, wherever, whenever) depends on dedicated Internet connectivity. Military installations are implementing smart grid technology as microgrids. On the other hand and more optimistically there are a number of initiatives to enhance security for new (not legacy, though) systems such as the Advanced Metering Infrastructure (AMI).

[16] Classified report published June 2012. Portions reproduced here are marked unclassified in the source report.

(network) components. While many engineers receive IT training it is often not as extensive as for an IT professional, and typically centers on operational rather than security aspects.

- Misconception 3: **All ICS Systems are Air-Gapped and Therefore Secure**.

Discussion: Not only is this not true (and actually never was even when most systems were isolated), but more and more systems that *were* air-gapped are being connected. Even air-gapped[17] systems are vulnerable, as demonstrated acutely by Stuxnet. Typically air-gapped systems still have connectable access points, such as the USB drive in the Stuxnet case. Additionally, when upgrades are made they may be by a CD that has not been properly scanned for viruses or by a vendor plugging an unscanned laptop into an Ethernet port. Not only is "air gapped" not necessarily secure, but dangerously can create a false sense of security (lends to the "security by obscurity" fallacy). Yet another facet of this is that the "isolated" system often is overlooked or even intentionally ignored during security audits that focus on the IT or network elements.

- Misconception 4: **ICS & SCADA Systems are Physically Secure.**

Discussion: Perhaps most of those directly under control of DOD are physically secure (though that has been shown to be false numerous times), but those not under DOD control are less likely to be secure, at least to DOD standards. The Government Accountability Office (GAO) estimates that 85% of energy infrastructure is "outside the fence" and that 99% of DOD's energy needs are met by commercial providers. Physical security (or lack thereof) does not end at the fence. In other words, no matter how physically secure the installation may be there are still external risks to be addressed. DOD dependence on commercial owners and providers demands a teaming approach to physical security.

- Misconception 5: **Proprietary Protocols Offer Security Through Obscurity.**

Discussion: "Proprietary" serves as an impediment only to those operating legally and ethically, and to a certain extent unsophisticated bad actors (only because they had not yet acquired the skills). To the experienced hacker and state-sponsored actor, protocols are discoverable and exploitable. There even have been web-published revelations of proprietary protocols by so-called independent researchers.

Misconceptions abound; therefore security may never be assumed or taken for granted. Any given installation's "most secure" ICS is fundamentally a function of continuous risk assessment and management relative to given missions and situationally-dependent mission priorities.

[17] "Air Gap" refers to having no electronic connection, requiring data to be moved "by hand" from one system to another via media such as USB drives, CDs, etc.

Continuous awareness is key to recognizing vulnerabilities early and committing necessary resources to manage potential risks. Proactivity is fundamental.

RISK ASSESSMENT & MANAGEMENT

Key Point:

- Risk management is a continuous process.

Risk is a function of the interaction among threat,[18] vulnerability, and consequence (or mission impact). Risk management involves a process of understanding each element of the equation, how those elements interact, and how to respond to the assessed risk. Every installation will face an ever-changing threat-vulnerability-consequence equation. SMEs within DOD, Department of Energy (DOE), and industry agree that even the most secure network has, or will have, inherent vulnerabilities. Therefore risk management is essential and must be a continuous process rather than an *event* that takes place annually, quarterly, or even monthly. Risk management is not only continuous but is situational based on the relative uniqueness of each ICS infrastructure. Appendix F *provides examples of risk assessment models.*

FRAMEWORK FOR SUCCESSFUL ICS DEFENSE

Key Point:

- ICS defense is a team effort.

While there is no DOD, Joint, or Service policy or directive specific to creating a security program for installation ICS, numerous publications do provide some guidance and address elements of ICS security. The following "best practice" framework is derived from such guidance.

1. Appoint a full-time ICS Information Assurance Manager (IAM) specifically for installation control systems (i.e., distinct from an IT IAM).[19] As an on-going coordinator of a team formed in the next step, the ICS IAM[20] will be responsible specifically for ICS and should function directly under the authority of the installation commander.

[18] "Threat" is further deconstructed into capability + intent + opportunity.

[19] Engineering Technical Letter (ETL) 11-1, released Mar 2011 by [then] HQ AFCESA/CEO, requires USAF CEs at base level to appoint both primary and alternate IAMs with a focus on certification & accreditation (C&A) of all CE-managed ICS. Note that AFCESA became AFCEC, of AF Civil Engineer Center, in October 2012.

[20] The ICS IAM should be officially designated, trained for the position, and delegated authority to immediately address issues within a defined sphere of responsibility. The ICS IAM should not be an additional-duty position.

2. Form an ICS security team led by the ICS IAM. Securing installation ICS networks cannot be fully accomplished by any single individual or necessarily by any single base entity (such as CEs or PWs typically considered "owners" of the infrastructure). Securing the ICS and reducing risk to mission must be a team effort. This team of authoritative experts should represent at least the CEs/PWs, the cyber unit, physical security, OPSEC, and missions operations. Engineers can inform the "what" and "where"; the cyber or communications experts can provide the "how"; and the mission representatives can explain the "why" as well as the consequences of failure. Intelligence producers can help understand the "who" that represents the threat. The installation commander sets priorities in the form of "when" and makes the critical decisions on commitment and allocation of resources and assets. Include other stakeholders as appropriate to the installation and mission set, such as when there are tenant organizations (e.g., hospital) whose missions may be distinct, but still rely on the installation ICS infrastructure.[21] Consider creating also as a sub-element of this team an ICS-Computer Emergency Response Team (CERT),[22] modeled on that led by Department of Homeland Security (DHS).[23] If a network CERT already resides on the installation, coordinate to include ICS.
3. Direct the ICS security team in identifying existing and/or developing new policies with respect to key elements of the ICS security program.
4. Promulgate policies and concurrently hold training sessions on the policies for all ICS users, operators, and maintainers (analogous: IA training for anyone who touches a network).
5. Implement policies and hold individuals accountable for adherence.
6. Assess effectiveness of measures undertaken (i.e., conduct risk analysis, exercise, red team, or/and tabletop review).
7. Monitor and adjust as needed.

Last resort: An IT IAM could have ICS added to their "job jar" but should receive additional training specific to ICS. Reference also ETL 11-1.

[21] (USAF) SAF/CIO A6, in a Memo dated 20 March 2012 (mandatory compliance) instructed installations to create a multi-disciplined Integrated Product Team (IPT) comprised of all stakeholders to assess IA of PIT, which includes control systems.

[22] CERT = Cyber Emergency Response Team.

[23] The DHS ICS-CERT website is found at http://www.us-cert.gov/control_systems/ics-cert/

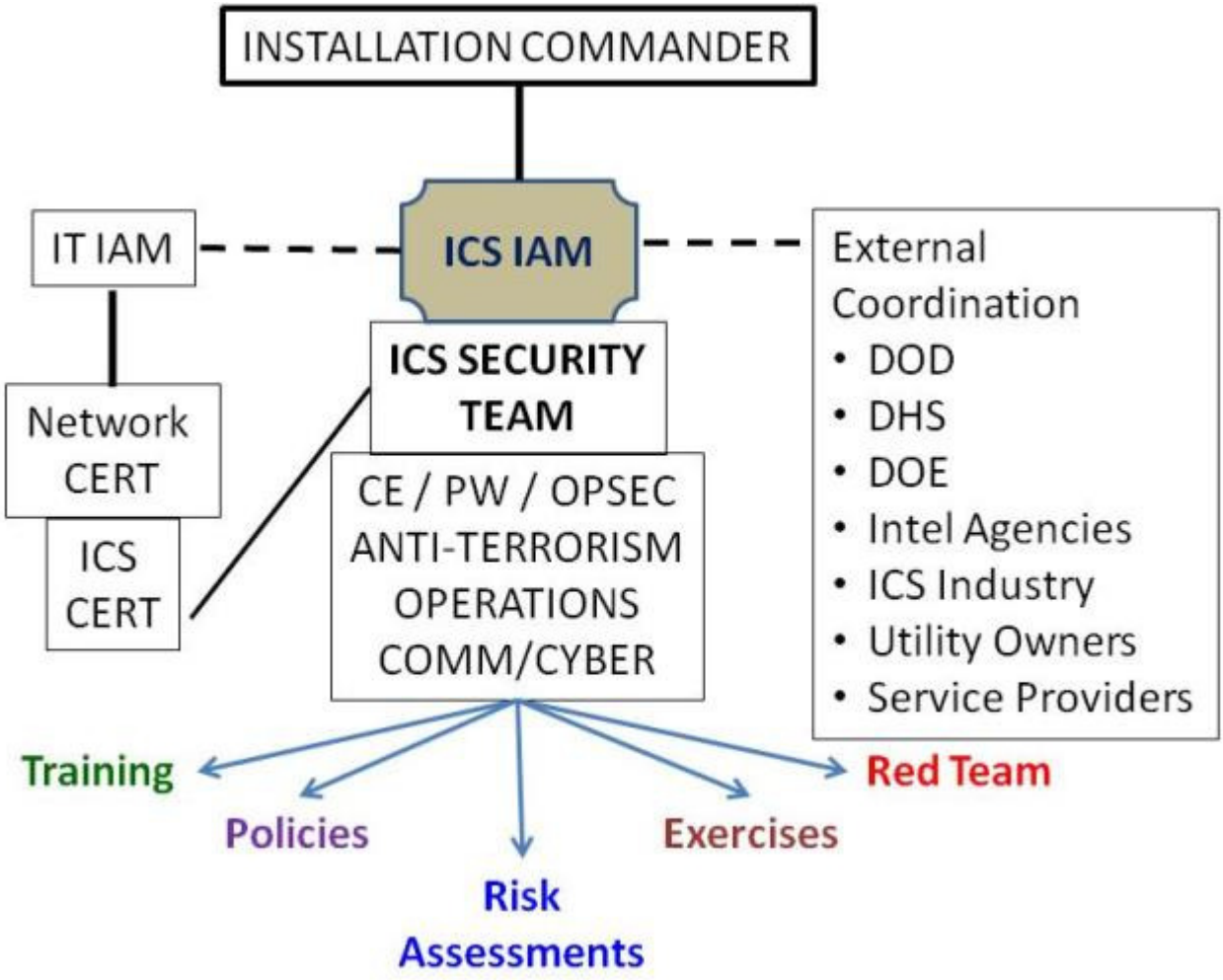


Figure 4. The ICS Security Team

"We also know [enemies] are seeking to create advanced tools to attack [control] systems and cause panic, destruction and even the loss of life."

Secretary of Defense Leon Panetta,
at a meeting in NY City
of Business Executives for National Security (Oct 2012)

ICS SECURITY ASSESSMENT PROCESS

Key Point:

- Must begin with missions analysis and prioritization.

The following eight-step process is the heart of this handbook. All other included information is in support of preparing for and understanding the criticality of the assessment process. Best practice is to follow the steps as presented, but individual circumstances may warrant reversing some steps and or accomplishing some in parallel. However approached, Step 1 must always be accomplished first.

While virtually every major entity engaged in ICS defense recommends some version of a "best" process for risk assessment and management, no two approaches are exactly the same. For example OPNAVINST 3500.39C on Operational Risk Management presents a 5-step process.[24] The approach presented here was developed by ICS SMEs working on the National SCADA Test Bed at Idaho National Laboratory (INL) and fits well with a DOD military installation focus.

In association with Step 7 of the process there is also a companion checklist of specific actions to consider. That checklist is found at Attachment 2 and is introduced by a textual section titled "Recommended Defense Actions."

Step 1. Mission analysis. For ICS defense, the task is to establish a baseline understanding among the stakeholders of the missions relative to the support infrastructure (both IT and ICS). A key product of this first step is a prioritization of missions that can be linked to assets and then ICS dependencies. Key question: If I have to devote all of my very limited resources to protecting one mission, what would that be? Then the one after that? Applying Mission Assurance Category (MAC) levels[25] can be useful to this endeavor. Also included may be a review of Mission Essential Tasks (MET)[26] with reference to the Defense Readiness Reporting System (DRRS). Mission analysis and decomposition, especially to a granularity useful to the rest of the steps, likely will not be a trivial process and may require significant commitment of the resource of time. A solid investment of time at this step will make the follow-on steps easier to accomplish.

[24] The OPNAVINST 5-step ORM process: Identify, Asses, Make decisions, Implement controls and Supervise, remembered by the mnemonic "I AM IS".
[25] MAC definitions found in the *Glossary*.
[26] MET examples in Appendix I.

Step 2. Identify assets. This includes not only direct mission assets (such as aircraft, tanks, ships, etc.) but more pointedly the infrastructure systems (such as fuels management and delivery) that support those. The key is to identify the thread from mission to asset to supporting infrastructure to ICS dependencies. This thread will reveal which ICS systems are more critical when it comes to applying security controls.

> "As a network defender, it is critical to know how the network is laid out as well as the hardware associated with the network. In order to defend SCADA, the operator needs to know what he or she has to work with."
>
> *AFTTP 3-1.CWO (para. 7.6.3.2)*

Step 3. Determine ICS connectivity. It is absolutely essential to identify every point of connectivity because the greatest vulnerability is at any point of connection. While NIPRNet connectivity may take top tier on the list, any connectivity—whether currently connected or *could be* connected later—must be identified. To leave even one *potential* connection undiscovered possibly is to leave the entire network[27] vulnerable. Running a scan on the network elements will identify only what is connected and on at the moment of the scan. This is a key reason for conducting a physical inventory as well, setting eyes on any and every potential connection capability. A PLC may be inside a locked cabinet inside a fenced compound with armed guards at a gate, but if it has an Ethernet port it is connectible (e.g., for vendor maintenance) and therefore, is a potential risk.

Step 4. Determine ICS dependencies. Which missions and their supporting infrastructure are dependent on a properly functioning control system? Are multiple control systems involved (as in the earlier example of traffic control, emergency systems, fuels delivery)? This step also requires technical network mapping typically coupled with a physical inventory and an operational-level understanding of the missions. See Attachment 1, *Mapping Interdependencies*, for an example methodology. A comprehensive approach to this must be followed with collaboration among representatives from at least the cyber, engineering, and mission operations communities.

Step 5. Assess risk. Risk is characterized as an outcome of the interaction among threat, vulnerability, and consequence. The goal is to gain a clear understanding of actual risks that can be managed. All stakeholders need to be engaged in every step of this entire process, but here is where collaboration becomes absolutely essential. Intelligence

[27] Arguably extreme, but since we do not know what we do not know (in this example) one is left contemplating "worst case."

analysts help identify external threats; engineer, PWs, and comm/IT specialists provide understanding of the control infrastructure and its vulnerabilities; and operations personnel can define the mission consequences or impacts of a realized threat event. Numerous risk analysis publications and external organizations are available to assist with this step.

Step 6. Prioritize risk management actions. Risk management typically entails deciding among a finite list of response options: avoid, share/transfer, mitigate, or accept. A response option or course of action (COA) typically is selected based on what is feasible, practical, and affordable (i.e., a cost-benefit analysis relative to mission impact). In most cases the commander, decides on a COA and then prioritizes commitment of resources to accomplish the actions.

Step 7. Implement actions. This step requires systematic implementation however simple or complex. At the minimum, one must identify the typical *who* is to do *what*, *where*, and *when*, i.e., direction, responsibility, accountability, and resources available. The *sine qua non* of implementation is commitment of resources combined with accountability mechanisms.

Step 8. Monitor, and reenter the cycle as required. This is never a "fire and forget" activity. Any (even trivial) change to an architecture can introduce new vulnerabilities (emphasizing also the imperative to institute a configuration control process). Additionally, threat actors are continuously on the hunt for vulnerabilities not yet discovered by legitimate owners and operators. To maintain a steady state of security requires continuous monitoring. Furthermore, implementation of any plan is likely to encounter impediments. This will be the phase or step to identify those and readjust as necessary. The success of this step depends on existence of feedback processes and mechanisms, which should have been implemented already.

SOFTWARE TOOLS

Key Point:

- Tools can be good or bad.
- Even a "good" tool is only as good as the expert who uses it.

For many steps in the process of assessing and defending security of ICS, there exists a broad selection of supporting primarily software tools. At the installation command level, it is important simply to note that while such tools are available, tools alone will not guarantee a successful defensive posture of ICS. The human element is essential in every step.

Perhaps **the most important** thing *to understand* about software tools used with or on any ICS is that the tool must not affect the operation of the ICS or, more specifically, the infrastructure it controls. The **most important** thing *to do* with respect to software tools is to defer to IT SMEs who already have a set of approved tools and understand potential impacts of using those tools on particular networks.

Because the services provided by critical infrastructure (electricity heading the list) must always be available, the ICS likewise must be always available. Therefore, any software-based assessment or forensics action upon or through the ICS must not impede, deny, or otherwise alter the system, the data throughput, or the services supported.

Because of the necessity of maintaining availability, due diligence must be exercised if considering use of traditional IT tools (scanners, penetration testers, etc.) on ICS networks. Some IT tools introduce negative effects on the ICS as well as on the controlled infrastructure. Examples are plentiful. The NIST SP 800-82 (p. 3-22) relates one such example:

> "A natural gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours."

While significant to those customers, this is trivial compared to impacts on national defense missions. For example, consider potential consequences if the same action involved an ICS supporting fuels management for a combat flying mission or life support systems at a hospital.

ADDITIONAL RESOURCES

Key Point:

- Outside help is available—and much of it is at no cost to the requestor.

Due primarily to the ever-changing nature of the ICS security landscape, published guidance tends to quickly become obsolete. Fortunately, beyond the array of formal publications there exists a helpful offering of additional useful resources. For example:

- Numerous web sites provide detailed information on ICS security issues, current threats, tools, etc. Some of the more prominent are provided as Appendix B, Web Links.
- Students at the Services' advanced Professionally Military Education (PME) schools can be exceptionally good sources for current insights as many engage in fresh research and produce theses specific to emerging ICS/SCADA issues.
- Industry conferences can be exceptional sources of lessons learned and/or best practices, as well as provide opportunity to network with experts.
- Finally, establishing a close relationship with local critical infrastructure owners (e.g., the electric power company, water provider, etc.) can yield better understanding of local threats and risks, and thus better security for the entire community.

For current threat assessment information, sources may include: Air Force Office of Special Investigations (AFOSI), the Army Criminal Investigative Division (CID), or other Service equivalent; intelligence analysts (the J2/A2/G2 shop); and the ICS-CERT's Alerts and Warnings.

ICS SECURITY ACTIONS

Key Point:

- Use this with Step 7 of the Process and with the tabular checklist provided as Attachment 2.

The following section presents a series of action recommendations for securing ICS. Numerous entities, to include DOD, DOE, Commerce Department, and commercial vendors have published similar lists (*see the "References" appendix for some of those*). These recommendations are augmented by the "stand-alone" tabular checklist found at Attachment 2, and most appropriately considered at Step 7 of the "Security Assessment Process."

The recommendations that follow are in an outline that follows the familiar doctrine, organization, training, materiel, leadership & education, personnel, facilities, and policy

DOTMLPF-P[28] framework[29] but with minor modification. The two modifications are that (1) doctrine (D) is not *directly* addressed[30] while (2) cyber security (C) has been added, resulting in a COTMLPF-P framework that exists only in this publication. "Cyber security" is used here to distinguish between those measures taken in, on and/or through the network(s) and those actions of a more or less physical nature (such as using access control lists). Arguably the most critical set of security measures, cyber security is addressed last because such measures are most effective when supported by solid implementation of actions in the other areas and in particular when guided by clear policy.

RECOMMENDED ICS DEFENSE ACTIONS

POLICY

"The **development of the organization's security policy is the first and most important step in developing an organizational security program**. Security policies lay the groundwork for securing the organization's physical, enterprise, and control system assets." [*Catalog of Control Systems Security*, DHS, Apr 2011, p. 4.] [*emphasis added*]

The National Security Agency (NSA), in its "Securing SCADA and Control Systems" brochure (referring to Sandia National Lab's *Framework for SCADA Security Policy*), states: "A Security Policy defines the controls, behaviors, and expectations of users and processes, and lays the groundwork for securing CS[31] assets. Since the acceptable use of CS is narrower and may have more demanding operational requirements than IT systems, they also **demand their own Security Policy**." [*emphasis added*]

The installation commander must establish authoritative and directive policies with regard to all other aspects of the ICS, thus the rationale for starting with the Policy area.

---

[28] DOTMLPF-P: doctrine, organization, training, materiel, leadership & education, personnel, facilities, and policy. This is borrowed from Chairman Joint Chiefs of Staff Instruction (CJCSI) 3170.01H, Joint Capabilities Integration and Development System (JCIDS); and further acknowledges DoDM 3020.45 Vol 2, Defense Critical Information Program (DCIP) Remediation Planning, which states that remediation planning "shall consider a full range of… [DOTMLPF] options".

[29] Examples of other frameworks: People, processes & technology; strategic, operational & tactical; management, operational & technical.

[30] Any action undertaken in any other area may lead to consideration of doctrinal change. However, this handbook facilitates practical application and so intentionally does not directly address doctrine. Ultimately, best practices may result in recommended changes to doctrine, requiring entering the JCIDS process.

[31] CS = NSA's abbreviation for "control systems."

Policy Actions

- Reuse policy where appropriate. Usually it is not necessary to start from scratch on every policy. Many ICS security issues are also IT and/or IA issues. Many published IT and IA policies may be adapted to ICS. Also, there is increasing promulgation of Service- and DOD-level policies specific to ICS (for example, Air Force Civil Engineering Support Agency[32] [AFCESA]'s ETL 11-1).
- Ensure policies are promulgated to the lowest user level, and require training programs to address ICS policies.
- With the ICS security team (discussed previously), determine which elements of the ICS require specific policies vs. those that may be combined into a single policy document. Examples:
  - An access control policy might include password management, physical facilities control, and connectivity controls.
  - A personnel security policy likely will warrant a dedicated policy document.
- Once complete, the set of policies should address at minimum:
  - Access control
  - Inventory accounting
  - Security of physical assets
  - Configuration control
  - Acquisition of new hardware/software
  - Patching of operating systems and programs
  - Vendor / third-party roles and responsibilities
  - Conduct of vulnerability and risk assessments

LEADERSHIP

Much is subsumed in "leadership." With regard to ICS security it is important that leadership remain engaged and that operators are confident there is a "top-down" emphasis on ICS security. Promulgation of policy is a critical start, but ongoing leadership gives life to those policies. Delegate requisite authority and demand accountability, but do not retreat from oversight.

Leadership Actions

- Conduct periodic awareness briefings to ICS operators and users. Recommend including quarterly reminders of potential threats.

[32] In October 2012 AFCESA merged with AFCEE and AFRPA to become AFCEC, or Air Force Civil Engineer Center. ETL 11-1 still validly exists as an AFCESA publication.

- Participate in ICS security stakeholder events, such as DOD conferences, industry group seminars, and on-line discussion forums.
- Establish collaborative relationships with commercial service providers (electric, water, gas, etc.), with focus on their security programs to secure the infrastructure beyond the installation fence. Invite them to training sessions as adjunct members of the security team.
- Identify and mitigate the conditions whereby reliance on vendors creates potential single points of failure. Vendors often are the ones most familiar with installation systems, do not always have immediate access to those systems, and at times can be denied access (such as during elevating FPCONs).
- Add ICS information to the Commander's Critical Information List.
- Engage in the ICS acquisition process from planning through installation; include upgrades to existing systems as well as new systems.
- Develop plans where none exist or otherwise incorporate ICS into those that do. Examples:
  - System Security Plan (SSP)
  - Continuity of Operations Plan (COOP)
  - Disaster Recovery Plan (DRP)
  - Contingency Plans–ICS operation under various INFOCON, FPCON, and other emergencies
  - Operations Security self-assessments and surveys

PERSONNEL

The human element is necessary for the successful operation of ICS, and therefore is a critical area. All individuals who operate, maintain, or otherwise access ICS must understand their respective roles and responsibilities and be appropriately trained to those responsibilities. The insider threat (legitimate operators with legitimate access but illegitimate intent) can overcome most security controls. Even an "honest broker" can make a mistake that results in the same (or worse) impact on mission that a true threat actor can cause.

Personnel Actions

- Ensure every individual is trained for their specific responsibilities and undergoes mandatory periodic update/refresher training (similar to IA training).
- Enforce access controls and establish consequences for violations. For example, every individual has a unique logon (best practice = role-based) and is allowed access only by that logon (i.e., no "guest" accounts).

- Require special background checks on individuals who have access to ICS elements that are critical to mission accomplishment. Consider requiring Secret clearances at least for those individuals with access to mission-critical elements and/or who have full system administration privileges.
- Request ICS managers and operators to sign confidentiality or non-disclosure agreements. Treat ICS information at the very least as unclassified but sensitive.
- Maintain rosters for physical access to facilities, such as rooms where servers are maintained. Require sign-in/sign-out when accessed.
- Create an ICS incident response team modeled on DHS' ICS-CERT.
- Ensure that personnel who resign, retire, or are fired do not have continued access to any element of the ICS. Extend this vigilance to employees of contractors and vendors.
- Ensure that relevant personnel (members of ICS security team, asset owners, etc.) either monitor or routinely are made aware of new vulnerabilities and incidents published by ICS-CERT and ICS component vendors.

TRAINING

Training includes formal, informal, and exercise. Many negative incidents involving ICS, the controlled infrastructure, and/or the missions they support are attributed to legitimate operators who made mistakes due to training deficiencies. A systematic program of mandatory training should be implemented for all managers, operators, and other users of the installation control systems.

Training Actions

- Ensure all operators (at minimum) have had ICS-specific training prior to granting access to any element or component.
- Require IA and OPSEC training for every individual accessing ICS computer systems even if those systems are not directly connected to the IT network. This training must also include contractors and vendors who only sometimes connect to ICS computer systems.
- Provide threat and vulnerability awareness via appropriate forums, unit security awareness training, workplace bulletin boards, etc.
- Exercise plans (incident response, disaster recovery, continuity of operations, etc). Include with other installation exercises where practicable and include ICS-related scenarios under elevating INFOCON and/or FPCON.
- Document all training and ensure each individual maintains currency.

ORGANIZATION

In many cases ICS tend to be "out-of-sight, out-of-mind" to all installation personnel but the CE or PW personnel. As long as the lights are on, water is running, and gates function properly there is no need to be concerned with the systems that make that true. The downside of this view is that it creates a dampening effect on responsibility and accountability for the total ICS infrastructure. While PW/CE accept "ownership" responsibility for the control system field elements, anecdotal information is that the IT side often is viewed as entirely under purview of the IT organization. Conversely, in some cases IT considers the entirety of the ICS network, including the front-end IT elements, as CE's responsibility.[33] The ICS must be considered as a mission-critical system of systems and treated as such organizationally, with collaboration among CE, IT, and the operations' stakeholders. Ill-defined division of labor (responsibility) can create gaps that become threat vectors, or the trade-space of threat actors (both internal and external).

Organization Actions

- Create a position for an ICS IAM with functional authority and direct access to the installation commander. Ensure the IAM's participation in key venues to provide commander advocacy for ICS security and awareness.
- Clarify (and document on command relationship charts) roles and responsibilities of PW/CE, communications, operations (and other stakeholders as appropriate) with respect to operation, maintenance, and security of installation ICS.
- Fully document the ICS—hardware, software, firmware, connectivity, and physical locations of all. Create a topology or ICS system map reflecting connections to supported missions and a logic diagram depicting all information/data flows.
- Assign responsibility for ICS configuration management and control. May require creation of a configuration control board (CCB). The key is this entity documents configuration and maintains continuing control over changes.
- Identify the entity/individuals responsible for developing formal plans (continuity of operations, disaster recovery, etc.).
- Establish roles and responsibilities with regard to third-party relationships.
- Ensure all ICS users and operators understand the chain of command particularly for incident reporting and response mechanisms.

[33] On a more positive note, the Air Force has made progress in resolving this issue. Implementation typically lags policy and direction but four key publications have been promulgated beginning in early 2011: SAF/CIO A6 memo of Feb 2011 appointing Designated Accrediting Authority for PIT (includes ICS); SAF/CIO A6 memo (Feb 2011) delegating Certifying Authority to AFCESA/CEO; AFCESA's ETL 11-1 (Mar 2011) which deals with ICS information assurance; and SAF/CIO A6 guidance memo (AFGM2.2, Mar 2012) addressing IA of all PIT and announcing commensurate changes to AFI 33-210.

FACILITIES

While some elements of the controlled infrastructure are of necessity exposed (for example the wires of the electric power grid, pipelines for natural gas) most of the control system elements are housed in facilities ranging from guarded buildings to remote access panels. Each type of facility engenders its own relatively unique security challenges, but all share the dichotomous requirement to ensure that legitimate users can gain quick access when necessary while at the same time exclude everyone else from any access whatsoever.

Facilities Actions

- Physically identify and visually inspect every facility that houses any element of the ICS, however seemingly insignificant. This includes fenced enclosures, buildings, rooms in buildings, field huts, lockboxes, panels, etc. Often overlooked but must be included in "facilities" are the physical connections (e.g., coaxial cable, digital subscriber line (DSL), fiber optics, telephone lines). On large installations it is especially important to identify, inspect, and secure any facility near the perimeter fence (where feasible, relocate away from perimeter).
- Ensure that cabling terminations and their housings are not overlooked. Threats can come from cutting, splicing, tapping, and/or intercepting.
- Develop a plan of action and milestones (POA&M) for addressing physical security deficiencies. An extremely high level of physical security may be achieved by placing cameras, alarms, and armed guards on every facility. However, this typically is neither practical nor cost-efficient. Focus should be on those ICS that are critical to the missions, and then emphasizing where the control system is most exposed to risk. Feasibility, practicality, and expense all will temper selected COAs.
- Create a map of the facilities and the assets housed by each. Use in training, exercises, and actual incident response.
- Ensure portable equipment (e.g., laptops) that may be in storage until required (for backups, recovery, etc.) is included in the inventory and security measures.
- Consider an OPSEC survey focused on ICS. In any event, OPSEC measures should be applied to appropriate elements.

MATERIEL

Consider how physical assets are acquired, maintained, and removed from service. Does policy or other guidance exist? Historically control systems have had a life cycle measured in decades as opposed to IT, which has a life cycle of three years or less. One outcome is that components that have built-in vulnerabilities can remain in the network for years, often without those

vulnerabilities and their attendant risks being addressed. Replacement and maintenance of ICS should be approached strategically (i.e., long-term) as well as tactically and operationally.

Materiel Actions

- Assign responsibility for oversight of the physical assets to a configuration control manager or board.
- Establish a formal process for acquisition of new components.
- Operationally test (including vulnerability assessment) proposed new components off-line before introducing into the live network. Collaborate with the National SCADA Test Bed (NSTB) entities (INL, Sandia National Laboratory [SNL]) to test components in "live" and simulated environments.
- Treat adjunct materials (software, tech manuals, SOPs, plans, schematics, etc.) with the same level of security as the ICS.

CYBER SECURITY

Cyber security for ICS is in many respects the same as for IT. Most front-end elements (e.g., servers, operating systems, human-machine interfaces, connectivity) are in fact information technology elements. On the other hand, since most non-IT components typically are on a 15-20 year refresh (replacement) cycle and are tied to the operating system with which they originally were installed, even the IT elements can "age-out" or become unsupported making cyber security at the front end more challenging. Differences from IT become more distinct "downstream" in the system, with RTUs, PLCs, and of course the field mechanisms (sensors, gauges, etc.) interfaced directly with the controlled infrastructure. Cyber security applies to all those elements because they are still part of the network. Nearly every component in the system could provide a threat vector into the network. Of primary concern is connectivity from/into NIPRNet and/or any segment of the GIG, but any connection into the system must be considered as creating a risk to the DOD missions of the installation.

> "Asset owners should not assume that their control systems are secure or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities."
>
> *ICS CERT-ALERT-12-046-01 (Feb 2012)*

This section reflects more actions, and more of them technology-based, than the other (D)OTMLPF-P areas. However, in spite of the expansion of information this listing should not be viewed as absolutely complete, finite, or prescriptive. Existing policies and procedures already in place and proven effective should not be replaced based solely on this listing. Consult other publications (see References), engage the IT and IA professionals, seek assistance/advice from other government-related ICS experts, and consider contracting for assessment services from commercial providers.

Cyber Security Actions

- Define and defend perimeters. "Defense in depth" is an operative phrase often encountered. Strategic approaches include creating enclaves, segmentation, and establishing demilitarized zones (DMZ), typically using firewalls. NSA, DHS, and others recommend total isolation of ICS networks but that is not always possible or practical. Where some connectivity is required, at least secure the points where connection can be made.
- Control web access. Where Internet or NIPRNet connectivity is required limit access to the web by turning off unnecessary web services and ports, and consider using "white" and/or

"black" lists of allowed/not allowed sites. (Note: Whitelisting is often preferred over blacklisting.)

- Protect data. Encrypt mission-critical data in transmission and provide backups or other redundancies for data in stasis (files, databases, etc.). As a caveat, downstream data such as between a PLC and a field device cannot be encrypted.
- Protect the operating system. Perimeter defense is a good start, but threat actors (insiders, for example) can find ways inside the perimeter. Use defensive tools[34] (software) such as for intrusion detection. Implement and update virus-checking software (may need to do manually if not connected). Establish a patching protocol (typically requires testing off-line first). Enable audit logging, and review the logs frequently to detect anomalous (especially illegitimate) activity. Also, remove all services, programs, etc. not needed for operation of the ICS.
- Manage installation of new assets. Ensure hardware and software factory default or contractor-enabled settings are changed. Do not allow anything that is connected/connectable, new or legacy, to be accessed using default passwords. Vendors prefer to maintain defaults especially on field devices (e.g., PLCs) for ease of maintenance access. Those same defaults typically are publically accessible, often published on vendor company web sites, and will be used by threat actors.
- Disable every connection point not needed. Points include USB ports, wireless access points, Ethernet jacks, satellite receivers, modems, etc. Provide positive control over all remaining points, ensuring no "backdoor" exists. Even one unguarded USB port can provide a devastating threat vector. This point is demonstrated by the publically reported outcome of the Stuxnet infection of an Iranian nuclear processing facility's centrifuge control system.
- Control individual access to all elements. The operating system server and workstations are obvious control points but some field elements such as PLCs can (and do) have separate logons. There are a number of operational and tactical actions to take, selectively or collectively. Foremost is to require each individual to have a unique (unshared) logon ID and password.[35] Policy should strictly prohibit shared passwords. Institute least-privilege and role-based access. Absolutely nothing should be accessible via "guest" or anonymous accounts, in spite of very plausible rationale for such given by vendors. Administrator privileges should be given to vendors only as required and then closely monitored.

[34] Discussed elsewhere, but a reminder is warranted: Be cautious with software tools. Some very effective tools for IT networks can cause problems on ICS. Typically, passivity is the key characteristic. Tools that interact with the system, such as for intrusion protection mostly, are to be avoided. If an interactive tools is determined to be necessary it must first be tested off-line before use on ICS. Even if it "passes" the test, tools should be closely monitored for unanticipated, undiscovered negative effects.

[35] Air Force is implementing Public Key Infrastructure (PKI) as widely as possible. Also, DoD-wide many logons are accomplished with a Common Access Card (CAC). Aside from the method of network access, the key takeaway is unique, linked to a vetted user, not shareable with anyone else.

Figure 5. It Only Takes a Minute

APPENDIX A REFERENCES

262 NWS, *Assessment of ICS Safe Harbor on Altus AFB*, 2010.

AFI 10-710, *Information Operations Condition (INFOCON)*, 2006.

AFI 32-1063, *Electric Power Systems*, 2005 [certified current 2010].

AFI 33-112, *Information Technology Hardware Asset Management*, 2011.

AFI 33-200, *Information Assurance Management*, 2008 [change 2, 2010].

AFI 33-210, *Air Force Certification and Accreditation Program*, [with attached SAF/CIO A6 guidance memo, AFGM 2.2, 2012, on the AFCAP] 2008.

AFMAN 33-282, *Computer Security (COMPUSEC),* 2012.

AFNIC, EV 2010-08, *Guide for Submission of Platform Information Technology (PIT) Determination Concurrence Requests*, 2010.

AFPD 10-24, *Air Force Critical Infrastructure Program (CIP),* 2006.

AFPD 32-10, *Installations and Facilities*, 2010.

AFPD 33-2, *Information Assurance (IA) Program*, 2007.

AR 25-2, *Information Assurance*, (Revised) 2009.

CJCSI 3209.01, *Defense Critical Infrastructure Program,* 2012.

CJCSI 6510.01F, *Information Assurance and Support to CND*, 2011.

CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*, 2006.

CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*, 2012.

CNSSI 4009, *National Information Assurance (IA) Glossary*, 2010.

CNSSP 22, *Policy on Information Assurance Risk Management for National Security Systems*, 2012.

DHS, *Catalog of Control Systems Security: Recommendations for Standards Developers*, 2011.

DHS, *Cross-Sector Roadmap for Cybersecurity of Control Systems*, 2011.

DHS, *Common Cybersecurity Vulnerabilities in ICS*, 2011.

DHS, *Cyber Security Assessments of Industrial Control Systems*, 2010.

DHS, *Cyber Security Procurement Language for Control Systems*, 2009.

DHS, *Primer: Control Systems Cyber Security Framework and Technical Metrics*, 2009.

DHS, *Recommended Practice*: *Creating Cyber Forensics Plans for Control Systems*, 2008.

DHS, *Recommended Practice: Developing an ICS Cybersecurity Incident Response Capability*, 2009.

DHS, *Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, 2009.

DHS, *Recommended Practices for Securing Control System Modems*, 2008.

DHS, *Risk Lexicon*, 2010.

DISA, *DOD Internet-NIPRNet DMZ Increment 1, Phase 1: Technology Overview*, 2011.

DISA, *Enclave Security Technical Implementation Guide* (STIG), 2011.

DOD, *Risk Management Guide for DOD Acquisition, Sixth Edition,* 2006.

DODD 3020.26, *Department of Defense Continuity Programs*, 2009.

DODD 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure*, 2010.

DODD 5205.02E, *DoD Operations Security (OPSEC) Program*, 2012.

DODD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)*, 2004 [certified current as of 2007].

DODD 8500.01E, *Information Assurance*, 2007.

DODD 8570.01, *Information Assurance Training, Certification, and Workforce Management*, 2004 [certified current as of 2007].

DODI 2000.12, *DOD Antiterrorism (AT) Program*, 2012.

DODI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*, 2008.

DODI 4170.11, *Installation Energy Management*, 2009.

DODI 5205.13, *Defense Industrial Base Cyber Security/Information Assurance*, 2010.

DODI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program*, 2007.

DODI 6055.17, *DOD Installation Emergency Management (IEM) Program*, 2010.

DODI 8500.2, *Information Assurance (IA) Implementation*, 2003.

DODI 8510.01, *Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)*, 2007.

DODI 8551.1, *Ports, Protocols, and Services Management (PPSM)*, 2004.

DODI 8582.01, *Security of Unclassified DOD Information on Non-DOD Information Systems*, 2012.

DODM 3020.45, Vol. 1, *Defense Critical Infrastructure Program (DCIP): DOD Mission-Based Critical Asset Identification Process (CAIP)*, 2008.

DODM 5205.02-M, *DoD Operations Security (OPSEC) Program Manual*, 2008.

DOE, *21 Steps to Improve Cyber Security of SCADA Networks*, 2002.

DOE, *Electricity Sector Subsector Risk Management Process (draft for public comment)*, 2012.

DOE / PNNL-20376, *Secure Data Transfer Guidance for Industrial Control and SCADA Systems*, 2011.

DON (Dept. of the Navy), *CIO Memo 02-10, Information Assurance Policy Update for Platform Information Technology*, 2010.

ETL 11-1, [USAF] *Civil Engineer ICS Information Assurance Compliance*, 2011.

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, 2006.

HSPD 7, *Critical Infrastructure Identification, Prioritization, and Protection*, 2003.

IEEE C37.1, *IEEE Standard for SCADA and Automation Systems*, 2008.

INL/EXT-07-12635, *Recommended Practice for Securing Control System Modems*, 2008.

INL/EXT-08-13979, *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program*, 2008.

INL/EXT-10-18381, *NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses*, 2010. (Reissued in 2011 as *Vulnerability Analysis of Energy Delivery Control Systems.)*

ISO 31000, *Risk Management–Principles and Guidelines*, 2009.

ITL Bulletin 8/11, *Protecting ICS–Key Components of Our Nation's Critical Infrastructures*, 2011.

JP 3-27, *Homeland Defense*, 2007.

JTF CapMed Inst. 8510.01, *Information Technology (IT) Platform Guide*, 2011.

MCO 3501.36A, *Marine Corps Critical Infrastructure Program (MCCIP),* 2008.

NERC CIPs 002-009, *Critical Infrastructure Protection Series.* (Version 4 released 2012; version 5 in review process.)

NIST Interagency Report 7435, *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems*, 2007.

NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*, 2011.

NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, 2010.

NIST SP 800-39, *Managing Information Security Risk*, 2011.

NIST SP 800-40, V.2, *Creating a Patch and Vulnerability Management Program*, 2005.

NIST SP 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*, 2009.

NIST SP 800-53, Rev. 4, *Security & Privacy Controls for Federal Information Systems and Organizations*, 2012.

NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, 2010.

NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide (Draft)*, 2012.

NIST SP 800-82, *Guide to Industrial Control Systems Security*, 2011.

NIST SP 800-92, *Guide to Computer Security Log Management*, 2006.

NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems*, 2007.

NSA, *A Framework for Assessing and Improving the Security Posture of Industrial Control Systems,* 2010.

NSTB, *NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses*, 2010.

SECNAVINST 3501.1B, *Department of the Navy Critical Infrastructure Protection Program*, 2010.

SECNAVINST 5239.3A, *Department of the Navy Information Assurance (IA) Policy*, 2004.

SNL, Sandia Report SAND2004-4233, *A Classification Scheme for Risk Assessment Methods*, 2004.

SNL, Sandia Report SAND2007-2070P, *Security Metrics for Process Control Systems*, 2007.

SNL, Sandia Report SAND2010-5183, *Control System Devices: Architectures and Supply Channels Overview*, 2011.

US Army TM 5-601, *SCADA Systems for C4ISR Facilities*, 2006.

APPENDIX B WEB LINKS

262 NWS	http://washingtonairguard.org/194rsw/
346 TS [CAC required]	https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=sF575FC8E22DC74AF01230B02FDC91C2B
AFCESA	http://www.afcesa.af.mil/ *Note that AFCESA became AFCEC in October 2012*.
CSET (DHS)	http://www.us-cert.gov/control_systems/satool.html
DTIC	http://www.dtic.mil/dtic/
DUSD (I&E)	http://www.acq.osd.mil/ie/
DOE / Energy.gov	http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011 "Roadmap to Achieve Energy Delivery Systems Cybersecurity"
DOE / Energy.gov	http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp Cybersecurity Risk Management process
ICS-CERT (DHS)	http://www.us-cert.gov/control_systems/ics-cert/
ICS-CERT	http://www.us-cert.gov/control_systems/cstraining.html Control Systems Security Program (CSSP) Training opportunities
Idaho NL	https://inlportal.inl.gov/portal/server.pt/community/home/255
Interagency OPSEC Support Staff (IOSS)	http://www.ioss.gov [*requires DoD credentials, e.g., CAC, to access*]
JDEIS	https://jdeis.js.mil/jdeis/index.jsp?pindex=0 links to DOD and CJCS issuances
NIST	http://www.nist.gov/index.html
Pacific Northwest NL	http://www.pnnl.gov/

Sandia NL	http://www.sandia.gov/
	http://energy.sandia.gov/?page_id=5800
SCADA Test Bed	http://www.inl.gov/scada/
USACE	http://www.usace.army.mil/
Vulnerability Database	http://nvd.nist.gov/

APPENDIX C ACRONYMS

AFCEC	Air Force Civil Engineer Command [result of Oct 2012 merger of AFCESA, AFCEE and AFRPA]
AFCESA	Air Force Civil Engineer Support Agency [later AFCEC]
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFNIC	Air Force Network Integration Center
AFOSI	Air Force Office of Special Investigations
AFPD	Air Force policy Directive
AFTTP	Air Force Tactics, Techniques, and Procedures
AIC	availability, integrity, confidentiality [vs. IT systems' CIA]
AIS	automated information system
AMI	Advanced Metering Infrastructure
APT	Advanced Persistent Threat
AR	Army Regulation
AT	antiterrorism
AV	antivirus
CAC	common access card
CAIP	critical asset identification process
C&A	certification & accreditation
CCB	Configuration Control Board
CCDR	combatant commander
CE	civil engineer
CERT	Computer Emergency Readiness Team
CIA	confidentiality, integrity, availability [vs. ICS systems' AIC]
CID	Criminal Investigation Division
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJCSM	Chairman, Joint Chiefs of Staff Manual
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Pamphlet
COA	course of action
COOP	Continuity of Operations Plan
COTS	commercial off-the-shelf
CPNI	Center for the Protection of National Infrastructure
CS	control system *[NSA term]*
CSET	Cyber Security Evaluation Tool

CVSS	Common Vulnerability Scoring System
DCI	Defense Critical Infrastructure
DCIP	Defense Critical Infrastructure Program
DCS	Distributed Control System
DEP	data execution prevention
DHS	Department of Homeland Security
DIACAP	DoD Information Assurance Certification & Accreditation Process
DISA	Defense Information Systems Agency
DSL	digital subscriber line
DISLA	Defense Infrastructure Sector Lead Agent
DMZ	demilitarized zone
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODM	Department of Defense Manual
DOE	Department of Energy
DON	Department of the Navy
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership (& education), Personnel, Facilities, and Policy
DRP	Disaster Recovery Plan
DRRS	Defense Readiness Reporting System
DTIC	Defense Technical Information Center
DUSD	Deputy Under Secretary of Defense
EMCS	Energy Management Control System
EMS	Emergency Medical Services
ETL	Engineering Technical Letter
FIPS	Federal Information Processing Standards
FPCON	Force Protection Condition
GAO	Government Accountability Office
GIG	Global Information Grid
GIS	geographical information services
HIPS	McAfee Host Intrusion Prevention System
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation and Air Conditioning
IA	information assurance
IAM	Information Assurance Manager
ICS	Industrial Control Systems [*US Army has used ICS also for "Instrumentation Communication Subsystem*"]

ICS-CERT	ICS Cyber Emergency Response Team
IDART	Information Design Assurance Red Team
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IEM	Installation Emergency Management
INFOCON	Information Operations Condition
INL	Idaho National Laboratory
IPS	intrusion prevention system
IPT	Integrated Product Team
IS	information system
ISO	International Organization for Standardization
ISP	Internet service provider
ISSM	Information System Security Manager
IT	information technology
JCIDS	Joint Capabilities Integration and Development System
JDEIS	Joint Doctrine, Education, and Training Electronic Information System
JIT	just in time *[refers to a just-in-time compiler]*
JP	Joint Publication
JTF	Joint Task Force
JWAG	Joint Warfighter Advisory Group
LUA	least user access
MAC	Mission Assurance Category
MCCIP	Marine Corps Critical Infrastructure Program
MCO	Marine Corps Order
MEF	mission essential functions
MET	mission essential task
MMS	multimedia messaging service
NERC CIPS	North American Electric Reliability Council Critical Infrastructure Protection Series
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTB	National SCADA Test Bed
OPNAVINST	Office of the Chief of Naval Operations Instruction
OPSEC	operations security
OSI	open system interconnect
OT	operational technology
PIT	Platform Information Technology (*includes ICS*)

PIT-I	PIT Interconnect [*refers to PIT connected to IT network*]
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PME	Professional Military Education
PNNL	Pacific Northwest National Laboratory
POA&M	Plan of Actions & Milestones
PW	public works
RBAC	role-based access control
ROP	return-oriented programming
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SECNAVINST	Secretary of the Navy Instruction
SMB	server message block
SME	subject matter expert
SMS	short message service
SNL	Sandia National Laboratory
SOP	standard operating procedures
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TM	Technical Manual
UAC	user access control
USACE	United States Army Corps of Engineers
USB	Universal Serial Bus
USSTRATCOM	United States Strategic Command
VoIP	voice over Internet Protocol
VPN	virtual private network
WAF	web application firewall

APPENDIX D GLOSSARY

Advanced Persistent Threat. An adversary that possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. [**NIST SP 800-53 Rev 4**]

- Advanced: The actor is adaptive and able to evade detection and is able to gain and maintain access to protected networks and resident sensitive information.
- Persistent: The actor has a strong foothold in/on the target network and is exceptionally difficult to completely remove or deny even if detected.
- Threat: The actor has both capability and intent that is counter to the best interests of the network and/or the legitimate users.

Asset. A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations. [**DODD 3020.40**]

Configuration Control. Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation. [**NIST SP 800-53**]

Defense Critical Infrastructure (DCI). DCI is the DOD and non-DOD networked assets essential to project, support, and sustain military forces and operations worldwide. Assets are people, physical entities, or information. Physical assets would include installations, facilities, ports, bridges, power stations, telecommunication lines, pipelines, etc. The increasing interconnectivity and interdependence among commercial and defense infrastructures demand that DOD take steps to understand and remedy or mitigate the vulnerabilities of, and threats to, the critical infrastructures on which it depends for mission accomplishment. The DCIP is a fully integrated program that provides a comprehensive process for understanding and protecting selected infrastructure assets that are critical to national security during peace, crisis, and war. It involves identifying, prioritizing, assessing, protecting, monitoring, and

assuring the reliability and availability of mission-critical infrastructures essential to the execution of the NMS. The program also addresses the operational decision support necessary for CCDRs to achieve their mission objectives despite the degradation or absence of these infrastructures. [**Joint Publication 3-27**] [*see also*: DODD 3020.40, DODI 3020.45, and DODM 2020.45 vols 1-5]

Defense-in-Depth. Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. [**NIST SP 800-39**]

Disaster Recovery Plan (DRP). A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. [**NIST SP 800-82**]

DOD Information Assurance Certification and Accreditation Process (DIACAP). The DOD process for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA controls, and authorizing the operation of DOD ISs, including testing in a live environment, in accordance with statutory, Federal, and DOD requirements. [**DODI 8510.01**]

Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail…Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. [**DODD 8500.01E**]

Force Protection Condition (FPCON). A Chairman of the Joint Chiefs of Staff-approved standard for identification of and recommended responses to terrorist threats against US personnel and facilities. [**Joint Pub 1-02**]

Incident. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies,

security procedures, or acceptable use policies. Incidents may be intentional or unintentional. [**NIST SP 800-82**]

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [**DODD 8500.01E**]

Information Assurance Manager (IAM). The individual responsible for the information assurance program of a DOD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the IA title Information Systems Security Manager (ISSM). [**DODI 8500.2**]

Information Operations Condition (INFOCON). The INFOCON system provides a framework within which the Commander USSTRATCOM (CDRUSSTRATCOM), regional commanders, service chiefs, base/post/camp/station/vessel commanders, or agency directors can increase the measurable readiness of their networks to match operational priorities. [**CJCSI 6510.01F**]

Intrusion Detection System (IDS). A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner. [**NIST SP 800-82**]

Intrusion Prevention System (IPS). A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. [**NIST SP 800-82**]

Mission Assurance. A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA; continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations. [**DODD 3020.40**]

Mission Assurance Category (MAC). Applicable to DOD information systems, the mission assurance category reflects the importance of information relative to the achievement of DOD

goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories: [**DODD 8500.01E**]

- MAC I. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.
- MAC II. Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.
- MAC III. Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

Mission Essential Functions (MEF). The specified or implied tasks required to be performed by, or derived from, statute, Executive Order, or other appropriate guidance, and those organizational activities that must be performed under all circumstances to achieve DOD component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly affect the Department of Defense's ability to provide vital services or exercise authority, direction, and control. [**DODD 3020.26**]

National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by

procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [**44 U.S.C., Sec. 3542**]

Platform Information Technology (PIT) and PIT-Interconnection (PITI). For DOD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or **essential in real time to the mission performance of special purpose systems** such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, **buildings**, and **utility distribution systems** such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration. [*emphasis added*] [**DODD 8500.01E, DODI 8500.2**]

Risk.

- Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. [**DHS Risk Lexicon**]
- A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [**CNSSI 4009**]
- An expression of consequences in terms of the probability of an event occurring, the severity of the event and the exposure of personnel or resources to potential loss or harm. A general expression of risk as a function of probability [P], severity [S], and exposure [E] can be written as: Risk = *f*(P, S, E). [**AFPAM 90-902**]

Risk Assessment. The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [**NIST SP 800-53**]

Risk Management. The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational

assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. [**NIST SP 800-53**]

Risk Management Strategies. [**DHS Risk Lexicon**]

- Acceptance: explicit or implicit decision not to take an action that would affect all or part of a particular risk.
- Avoidance: strategies or measures taken that effectively remove exposure to a risk.
- Mitigation: application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences.
- Transfer: action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area.

Risk Mitigation. Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. [**NIST SP 800-53**]

Security Audit. Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. [**NIST SP 800-82**]

Security Policy. Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent. [**NIST SP 800-82**]

System Security Plan (SSP). Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [**NIST SP 800-18**]

Supervisory Control and Data Acquisition (SCADA). A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. [**NIST SP 800-82**]

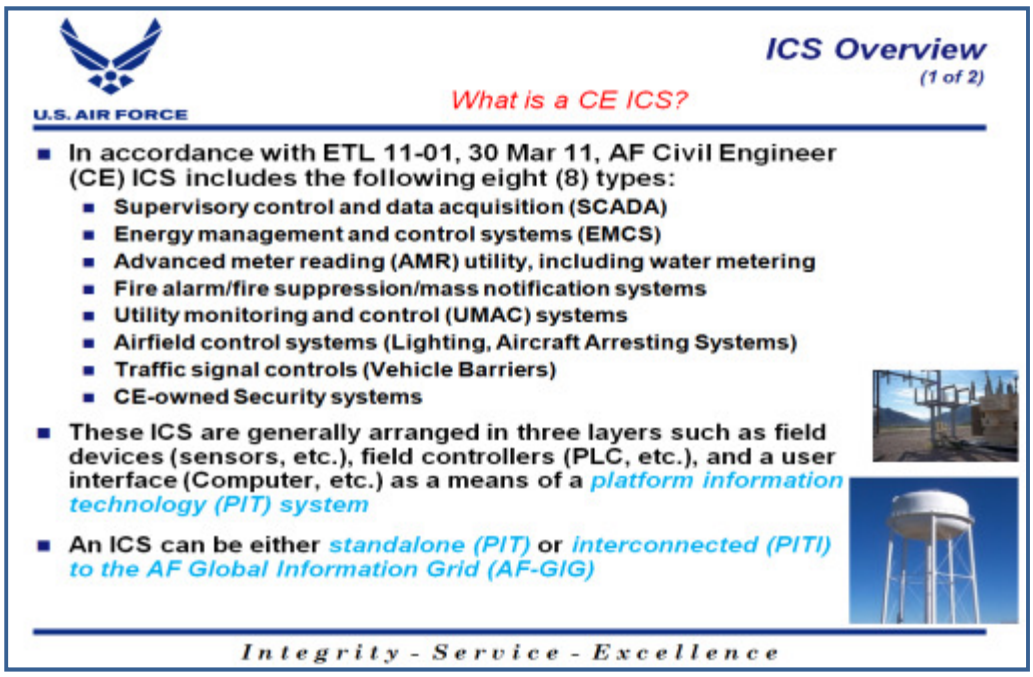
Task Critical Asset. An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DOD Components or DISLA organizations to execute the task or mission-essential task it supports. Task critical assets are used to identify defense critical assets. [**DODD 3020.40**]

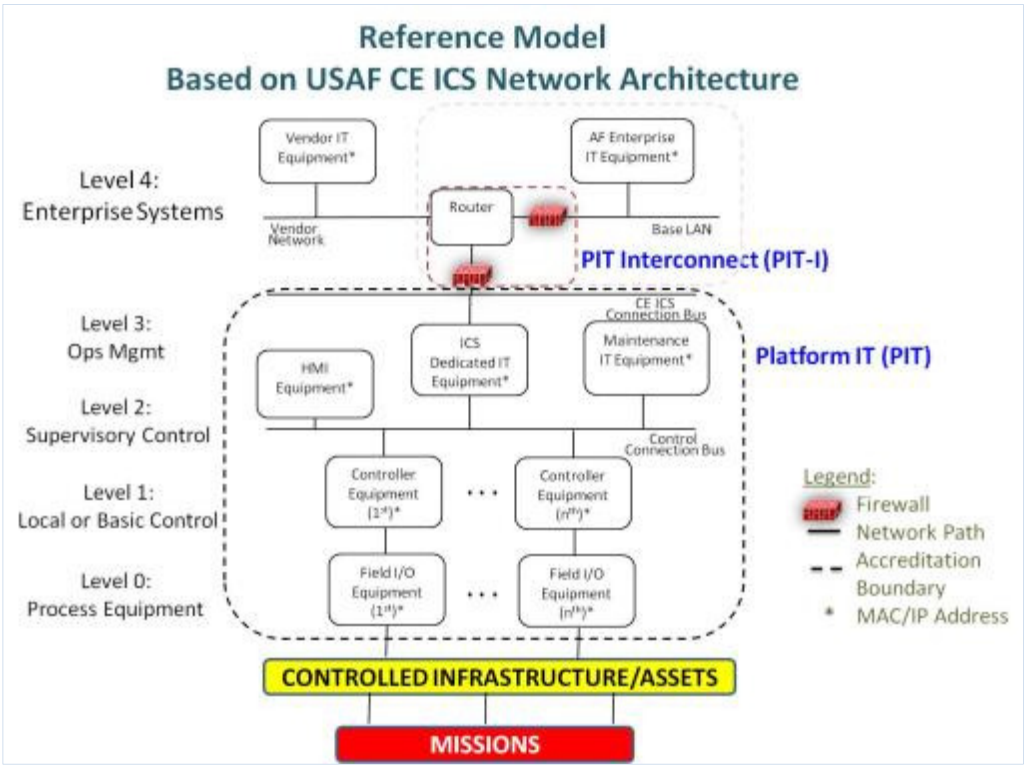
Virtual Private Network (VPN). A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. [**NIST SP 800-82**]

Vulnerability Assessment. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [**NIST SP 800-39**]

APPENDIX E CE BRIEFING GRAPHICS

The following two graphics were extracted from an AFCESA brief dated February 2012. (*The Reference Model is modified from the original*.) They are offered simply as representative of a Service view of ICS.





APPENDIX F RISK ASSESSMENT & MANAGEMENT MODELS

Extracted from selected publications as representative of varying approaches for modeling the basic process of risk management. Numerous varieties exist. Figures F1–F4 illustrate these varieties.

F1. DCIP Risk Management Process Model copied from DODI 3020.45, (p. 16).

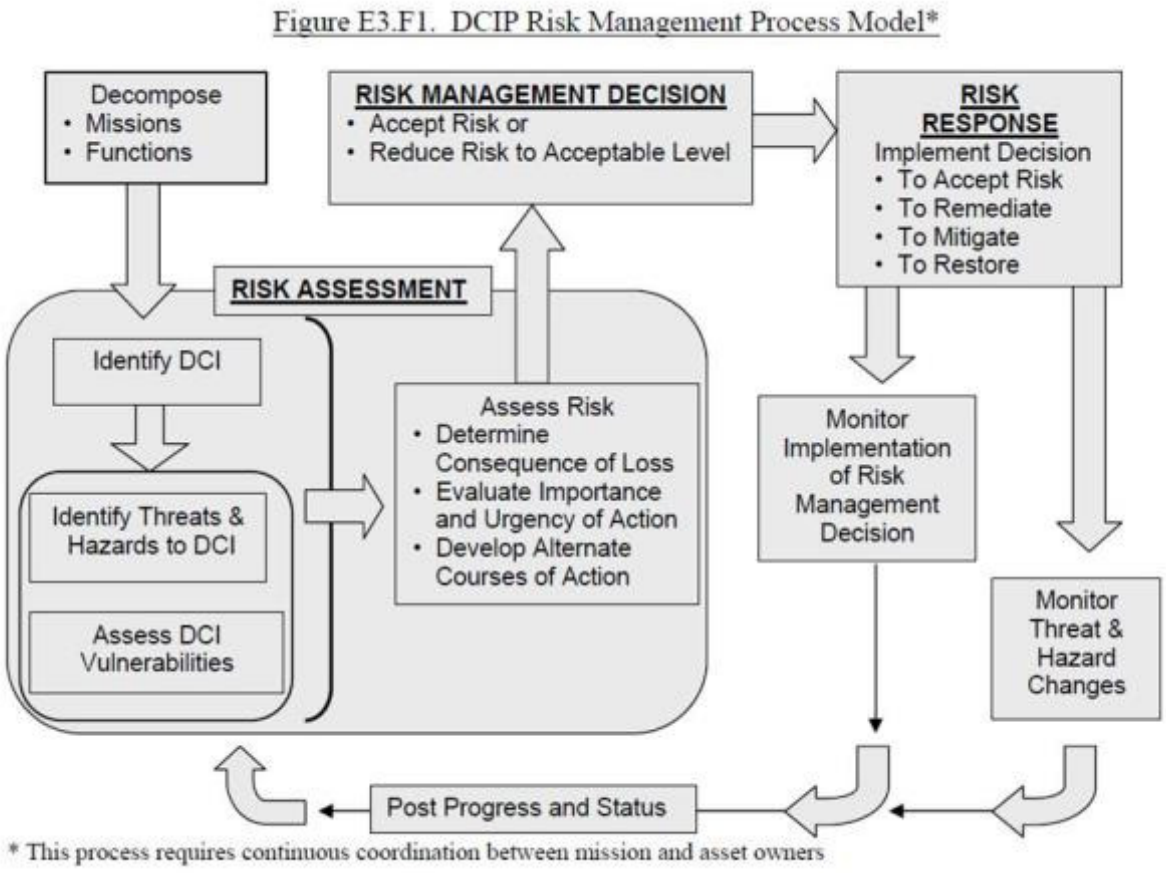


Figure F1. DODI 3020.45

F2. Risk Assessment Model as represented in NIST SP 800-30 (Rev. 1, Draft, 2011), (p. 7).

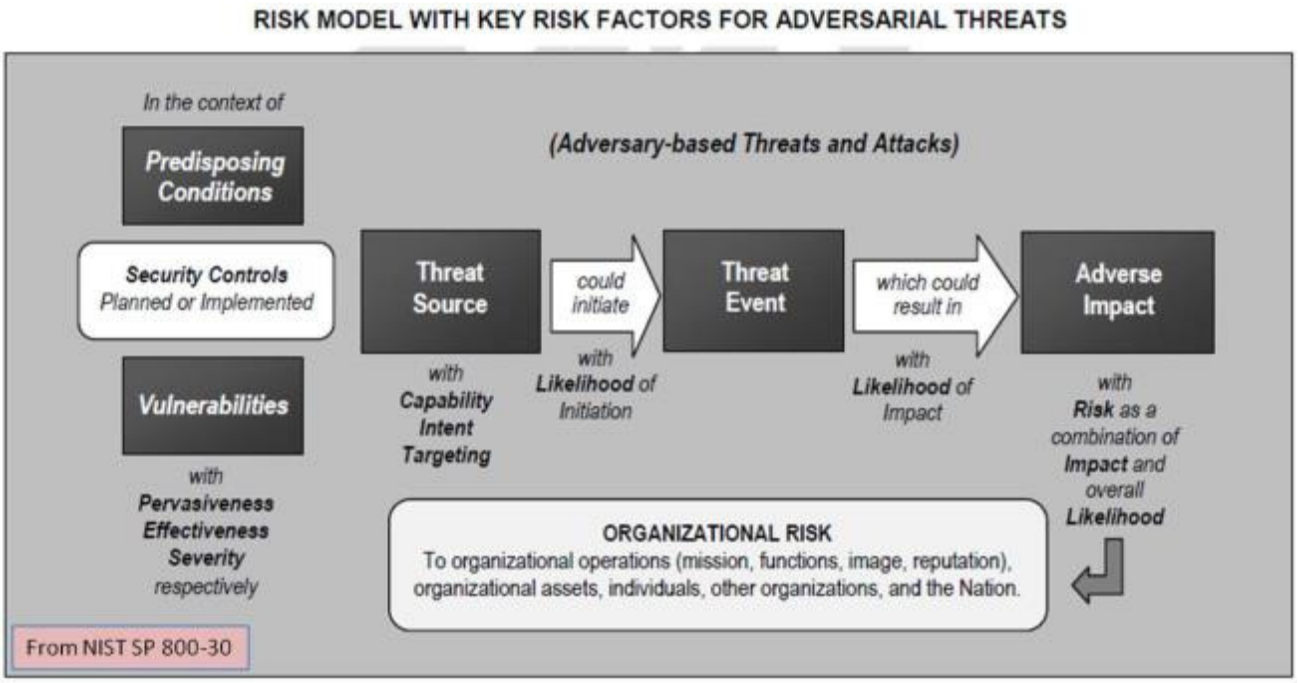


Figure F2. NIST SP 800-30

F3. Risk Management Process model depicted in ISO 31000, (p. 14).

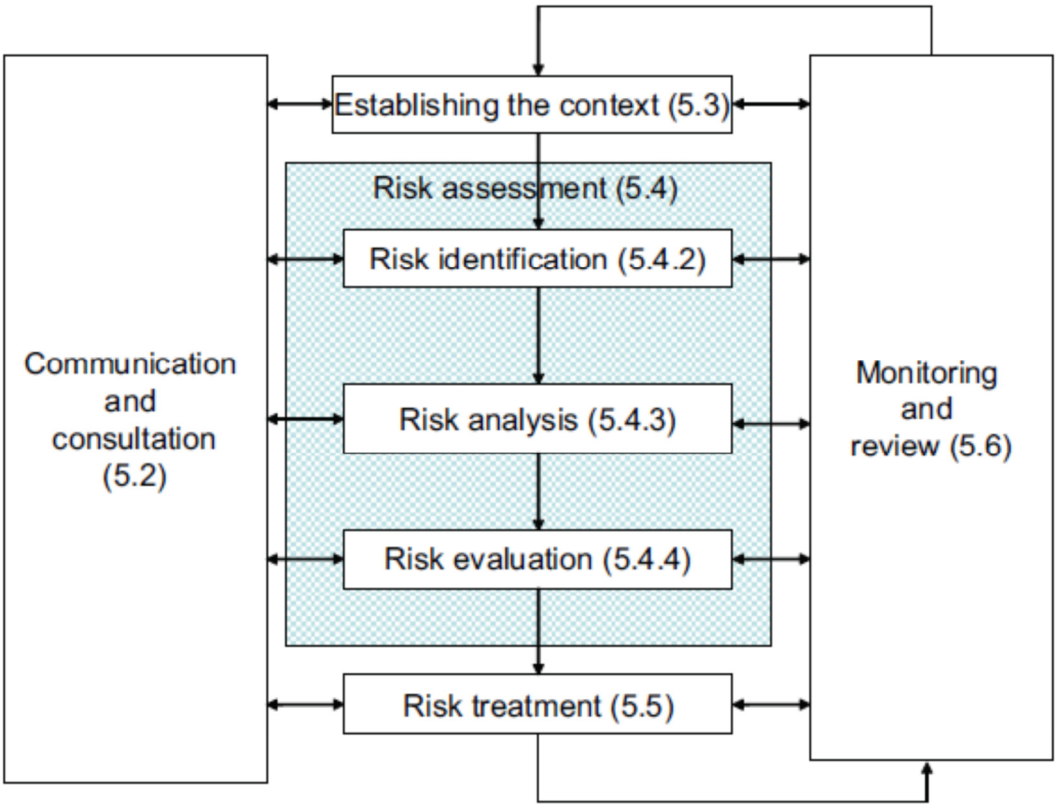


Figure F3. ISO 31000

F4. Generic model of risk assessment process.

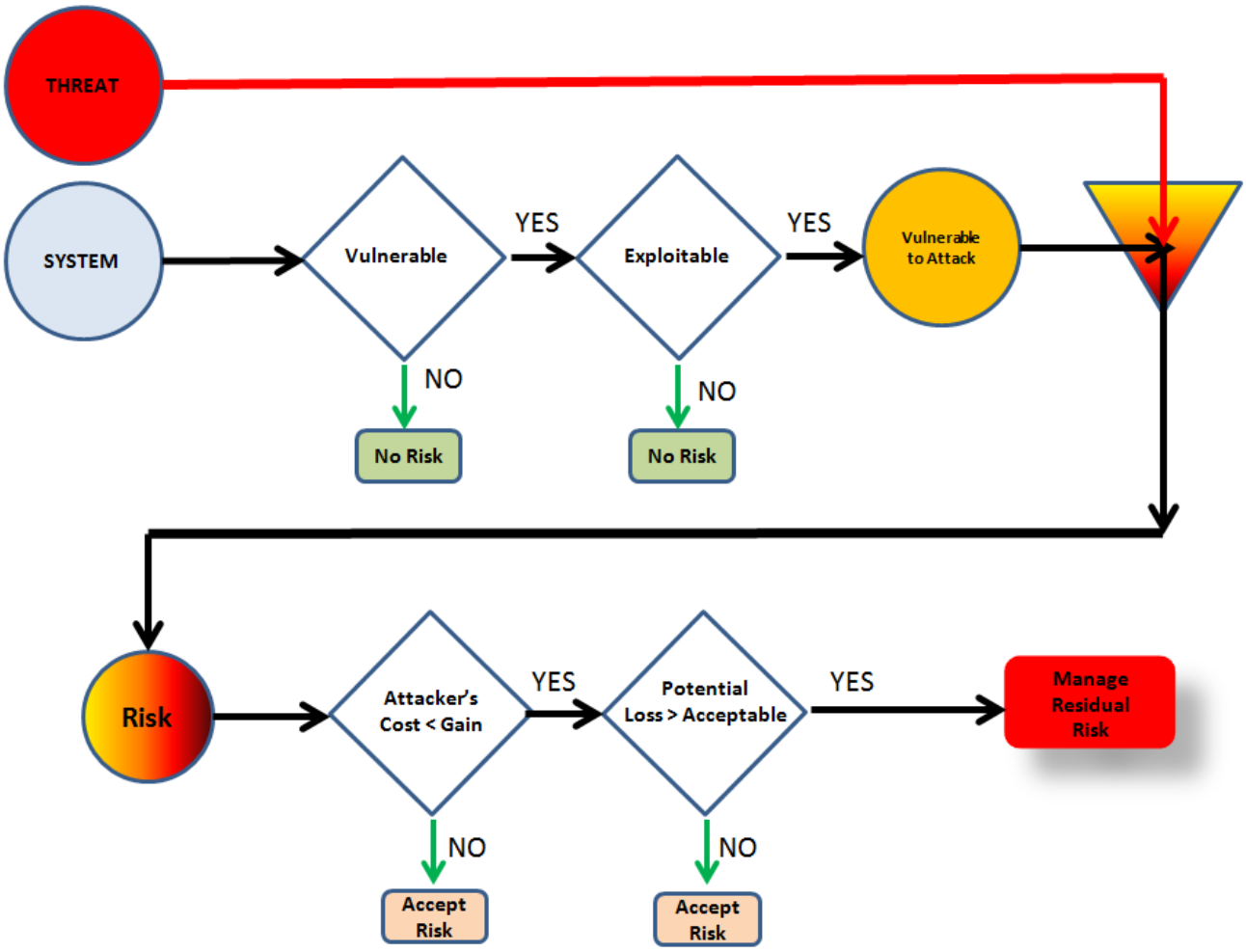


Figure F4. Generic Risk Assessment Process

APPENDIX G CSET

CYBER SECURITY EVALUATION TOOL (CSET)

[*Following extracted from the ICS-CERT web site*. http://www.us-cert.gov/control_systems/satool.html]

The Cyber Security Evaluation Tool (CSET™) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS National Cyber Security Division (NCSD) by cybersecurity experts and with assistance from the National Institute of Standards and Technology. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems. CSET is a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems. The tool derives the recommendations from a database of cybersecurity standards, guidelines, and practices. Each recommendation is linked to a set of actions that can be applied to enhance cybersecurity controls.

A caveat provided by the ICS-CERT: CSET is only one component of the overall cyber security picture and should be complemented with a robust cyber security program within the organization. A self-assessment with CSET cannot reveal all types of security weaknesses, and should not be the sole means of determining an organization's security posture. The tool will not provide an architectural analysis of the network or a detailed network hardware/software configuration review. It is not a risk analysis tool so it will not generate a complex risk assessment. CSET is not intended as a substitute for in depth analysis of control system vulnerabilities as performed by trained professionals.

SAMPLE QUESTION FROM CSET

Question 12. Is a disaster recovery plan prepared, tested, and available in the event of a major hardware or software failure or destruction of the facility? Check all that apply.

Result	Answer(s)
	Not answered
Fail	None of the controls are implemented.

Pass	A disaster recovery plan (DRP) is available and is tested.
	Critical replacements for hard-to-obtain components are kept in inventory.
	The DRP includes a communication procedure and list of personnel to contact in the case of an emergency including ICS vendors, network administrators, ICS support personnel, etc.
	The DRP includes a complete and up-to-date logical network diagram.
	The DRP includes an authorized personnel list of those required for the ICS operations and maintenance.
	The DRP includes current configuration information for all components.
	The DRP includes procedures for operating the ICS in manual mode until secure conditions are restored.
	The DRP includes process and procedures for backup and secure storage of information.
	The DRP includes required response to events that activate the recovery plan.
	The DRP includes roles and responsibilities of responders.
	The DRP indicates requirements for the timely replacement of components in the case of an emergency.

Level Specific Requirement: [*part of the sample question*]

A disaster recovery plan is essential to continued availability of the ICS. The DRP should include the following items: Required response to events or conditions of varying duration and severity that would activate the recovery plan; Procedures for operating the ICS in manual mode with all external electronic connections severed until secure conditions can be restored; Roles and responsibilities of responders; Processes and procedures for the backup and secure storage of information; Complete and up-to-date logical network diagram; Personnel list for authorized physical and cyber access to the ICS; Communication procedure and list of personnel to contact in the case of an emergency including ICS vendors, network administrators, ICS support personnel, etc.; Current configuration information for all components.

The plan should also indicate requirements for the timely replacement of components in the case of an emergency. If possible, replacements for hard-to-obtain critical components should be kept in inventory.

APPENDIX H DCIP

DEFENSE CRITICAL INFRASTRUCTURE PROGRAM (DCIP)

[*verbatim extract from the DCIP web site* http://dcip.dtic.mil/index.html]

DCIP is an integrated risk management program designed to support DOD Mission Assurance programs. When effectively applied, these programs form a comprehensive structure to secure critical assets, infrastructure, and key resources for our nation. The nation's defense and economic vitality is highly dependent upon the availability and reliability of both DOD and non-DOD owned critical infrastructure (such as: power, transportation, telecommunications, water supply, etc.). With limited resources to address risk to critical infrastructure, the DCIP relies on continuous analysis of changing vulnerabilities to all types of threats and hazards to effectively manage risk to the nation's most essential infrastructure.

Recognizing how critical the infrastructure is to accomplishing DOD's missions and the effects of vulnerabilities to threats and hazards of infrastructure assets, DOD Directive 3020.40, *DOD Policy and Responsibility for Critical Infrastructure,* established the Defense Critical Infrastructure Program (DCIP), a program responsible for coordinating the management of risk to the critical infrastructure that DOD relies upon to execute its missions.

Increased global connectivity and interdependencies create numerous and changing vulnerabilities. Threats to "soft" targets do not only occur through criminal or terrorist activities, but also through national disasters, accidents, hazardous weather, and other natural and man-made events. Our national military strength and economic vitality is highly dependent upon the availability and reliability of both DOD and non-DOD owned critical infrastructure (such as: power, transportation, telecommunications, water supply, etc.) However, resources to address these vulnerabilities are limited and must be channeled to those deemed the highest priority. Additionally, priorities change as threats, vulnerabilities, and mission requirements evolve.

Relevant publications include:
DODD 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure*
DODI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*
DODM 3020.45 Vol 1, *DCIP: DOD Mission-Based Critical Asset Identification Process (CAIP)*
DODI 5240.19, *Counterintelligence Support to the DCIP*
CJCSI 3209.01, *Defense Critical Infrastructure Program*
SECNAVINST 3501.1B, *Department of the Navy Critical Infrastructure Protection Program*
MCO 3501.36A, *Marine Corps Critical Infrastructure Program (MCCIP)*
AR 525-26, [Army] *Infrastructure Risk Management*
AFPD 10-24, *Air Force Critical Infrastructure Program (CIP)*

APPENDIX I UNIVERSAL JOINT TASKS

UJTs Relevant to Securing Critical Infrastructure

Universal Joint Tasks (UJT) provide the foundation upon which METs are constructed. The following selected UJTs are verbatim from the UJT List (UJTL) database found on the Joint Doctrine, Education & Training Electronic Information System (JDEIS).[36] The selection is not meant to be all-inclusive but representative and is provided merely to highlight the link between installation-level activities to secure ICS and national-level requirements.

SN 3.3.6.1 Assess Critical Infrastructure (CI) Impacts to Operational Capability
Determine the operational impacts resulting from the loss, disruption, and/or degradation of mission critical infrastructure.
Note: This task includes identifying the critical infrastructure and assets that are components of systems supporting all assigned missions; analyzing the potential consequences of a global event; assessing potential impacts to critical infrastructure and assets supporting assigned missions; and reporting results of the analysis and assessment.

SN 6.6.7.2 Conduct Defense Critical Infrastructure Program Analysis
To perform program management responsibilities including identification of defense critical infrastructures, perform risk analysis of vulnerabilities and mitigation, develop and maintain a predictive analysis capability to forecast and mitigate failure of critical assets early on. Seek input from the Defense Critical Infrastructure Program (CIP) sectors and report suspicious activities at specific facilities to appropriate Department of Defense and other governmental authorities.

ST 6.6.3 Manage Mission Risk Resulting From Defense Critical Infrastructure (DCI) Vulnerabilities
To manage actions taken at combatant command level to reduce the risk of mission degradation or failure, induced by known vulnerabilities of defense critical assets, infrastructure, or functional capability.

ST 6.6.4 Prevent or Mitigate the Loss or Degradation of Critical Assets
To allocate resources to reduce or offset asset vulnerabilities from all hazards, man-made, and natural threats.

[36] https://jdeis.js.mil/jdeis/index.jsp?pindex=43

ST 6.6 Perform Mission Assurance

Maintain plans and programs to ensure assigned tasks or duties can be performed IAW the intended purpose or plan.

Note: This task focuses on fully integrating a mission-focused process to understand and protect physical and information capabilities critical to performance of assigned missions at the strategic theater level of war. It links risk management program activities and security related functions -- such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear and high-explosive defense; readiness and installation preparedness -- to create the synergistic effect required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.

OP 6.7 Conduct Defense Critical Infrastructure Protection Program

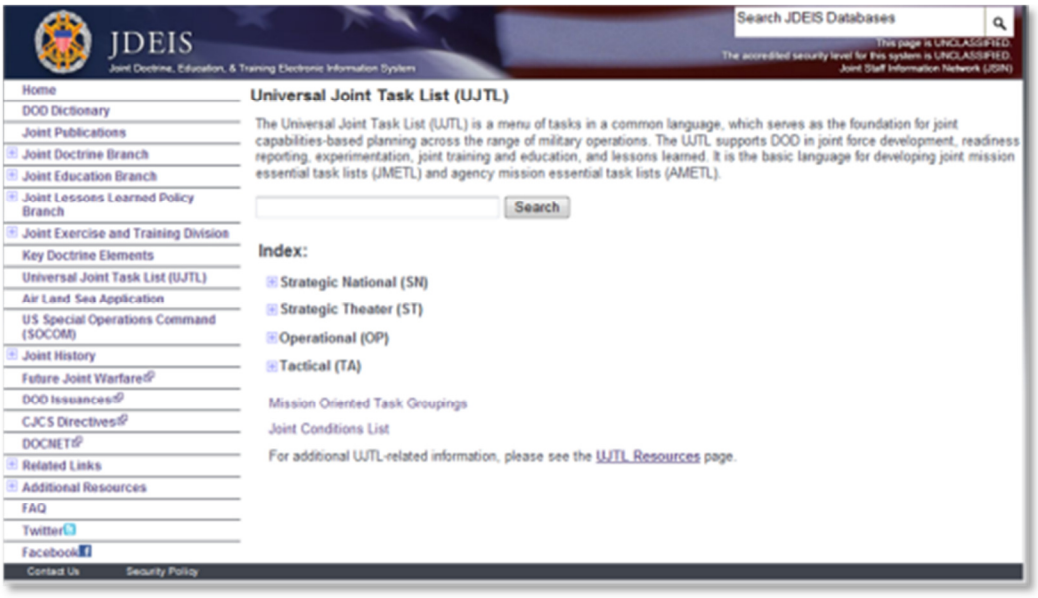
To conduct coordination between individuals charged with day-to-day operation and maintenance of DCI/As and the individuals charged with infrastructure investment strategies.

OP 6.7.1 Identify Task Critical Assets

To identify mission-critical assets and associate them with a particular facility.

OP 6.7.2 Coordinate Task Critical Asset Vulnerability Assessment

To conduct a systematic examination of mission-essential systems, assets, and applications, to identify vulnerabilities, which could cause a degradation or loss (incapacity to perform designed function) as a result of being subjected to a certain level of threat or hazard.



APPENDIX J ICS TRAINING OPPORTUNITIES

Training on various aspects of ICS to include security is available from numerous providers and in a variety of venues. The following samples are by no means all-inclusive but represent the variety of vendors and venues. Descriptions are from the vendors' or sponsors' web sites. For those not overly familiar with ICS, an excellent starting point is the US-CERT's web-based "Cyber Security for Control Systems Engineers & Operators" (link below). In spite of the course title, it is not necessary to be either an engineer or an ICS operator to gain valuable fundamental understanding about ICS security in a very short time.

US-CERT (http://www.us-cert.gov/control_systems/cstraining.html)

- **Web-based Training**
  The following summary level courses are available for on-line training:
  OPSEC for Control Systems
  Cyber Security for Control Systems Engineers & Operators
- **Instructor Led format - Introductory Level**
  Introduction to Control Systems Cybersecurity (101) - 1 day or 8 hrs
  ICS Security for Management (111) - 1 - 2 hrs
- **Instructor Led format - Intermediate Level**
  Intermediate Cybersecurity for Industrial Control Systems (201) - lecture only - 1 day or 8 hrs
- **Hands-on format - Intermediate Technical Level**
  Intermediate Cybersecurity for Industrial Control Systems (202) - with lab/exercises - 1 day or 8 hrs
- **Hands-on format - Advanced Technical Level**
  ICS Advanced Cybersecurity (301) - 5 days
- The Control Systems Security Program (CSSP) provides training courses and workshops at various industry association events. These courses are packed with up-to-date information on cyber threats and mitigations for vulnerabilities. I f your organization would like to learn more about training opportunities, please contact cssp_training@hq.dhs.gov.

Sandia National Laboratories (http://energy.sandia.gov/?page_id=6912)

SCADA Assessment Training Course: Methodologies for assessing SCADA systems and an overview of related security and vulnerability concerns

This customizable course covers a breadth of SCADA and other digital control system use in infrastructures and industry, identifies vulnerabilities of these components and systems, and presents methodologies and tools to assess these systems in a successful, measurable, reproducible manner. It is being offered to other groups on a limited basis in order to improve the security of infrastructures and systems critical to the United States. This

course is offered at Sandia's discretion to individuals with need-to-know and by invitation only.

Idaho National Laboratory (http://www.inl.gov/scada/training/)

The following courses are available through Idaho National Laboratory NSTB program. All the courses are designed to increase cyber security awareness and defensive capabilities for IT/Control System managers, IT/Control System security personnel, network and control system support engineers, and control system designers and developers who are involved in or responsible for control system cyber security. The courses are geared toward systems in the energy sector, but are relevant to most control system environments. The 4- and 8-hour courses are certified for NERC continuing education credits.

- Introductory SCADA Security (4 hours)
- Intermediate SCADA Security (8 hours)
- Advanced SCADA Security Red/Blue Team (5 days)

Air Force Institute of Technology
(http://www.afit.edu/CESS/Course_Desc.cfm?p=WTSS%20580)

COURSE: **WTSS 580 Managing Security of Control Systems**
OBJECTIVE: To assess vulnerabilities for control systems' environment for people, processes, and technology and recommend improved security strategies.
DESCRIPTION**:** This course explores a wide range of people, processes, and technology issues in the management of critical infrastructure control systems (CS) security including Supervisory Control and Data Acquisition (SCADA) systems security. Systems monitoring and controlling base-level and regional supply and flow of resources such as electricity, water, gas, and transportation are examined. Topics include CS components, threats, and vulnerability assessment and technical measures for improving security peculiar CS, such as multifactor authentication, telephony firewalls and radio frequency encryption, and operational and physical security. The CS industry and initiatives in CS security standards are explored. This includes focus on the interplay between regional commercial providers and base-level continuity of operations. The move toward integration of CS with traditional computer networks is covered.

INFOSEC Institute (http://www.infosecinstitute.com/courses/scada_security_online.html)

SCADA Security Online: SCADA, DCS, and other process control networks, generically called SCADA, run the nation's mission critical infrastructure, everything from the power grid to water treatment, chemical manufacturing to transportation. These networks are at increasing risk due to the move to standard protocols, the Microsoft OS and

interconnection to other networks. Learn the skills required to direct and manage the appropriate cyber security protection for your SCADA system.

SANS Institute (http://www.sans.org)

- **Intermediate SCADA Security: Department of Energy**: National SCADA Test Bed Program (Hands-on) - This fast-paced course covers general control system cyber security challenges. The training objectives include looking at the risk equation (threat, vulnerability and consequences) and how they relate to the control system environment. Who are the threat actors? What vulnerabilities exist in the control system space? What can be the consequences of exploitation? What mitigation strategies can be implemented to help protect the control system environment?
- **SCADA Security Advanced Training**: This five-day course combines advanced topics from SCADA and IT security into the first hands-on Ethical Hacking course for ICS. Both SCADA Administrators and IT Security Professionals will widen their knowledge through hands-on exercises with live SCADA systems and equipment.

Sampling of other vendors (*caveat emptor*):

- Lofty Perch (https://www.loftyperch.com/index/use_lang/EN/page/401.html)
- SCADAhacker (http://scadahacker.com/training.html)
- Red Tiger (http://www.redtigersecurity.com/)
- TONEX (http://www.tonex.com/Courses/194/1499/)
- Digital Bond (https://www.digitalbond.com)--but not accessible from .mil domain


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
SECURITY PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
ABOUT US
GFIRST
Control Systems
Home
Calendar
ICS-CERT
ICSJWG
Information Products
Training
Recommended Practices
Secure Architecture Design
Assessments
Standards & References
Related Sites
FAQ
Control Systems Security Program (CSSP)
Training available through CSSP
Scheduled training is on the CSSP Calendar.
Web-based Training
The following summary level courses are available for on-line training:
OPSEC for Control Systems
Cyber Security for Control Systems Engineers & Operators
Instructor Led format - Introductory Level
Introduction to Control Systems Cybersecurity (101) - 1 day or 8 hrs
ICS Security for Management (111) - 1 - 2 hrs
Instructor Led format - Intermediate Level
Intermediate Cybersecurity for Industrial Control Systems (201) - lecture only - 1 day or 8 hrs
Hands-on format - Intermediate Technical Level
Intermediate Cybersecurity for Industrial Control Systems (202) - with lab/exercises - 1 day or 8 hrs
Hands-on format - Advanced Technical Level
ICS Advanced Cybersecurity (301) - 5 days
The Control Systems Security Program provides training courses and workshops at various industry association events. These courses are packed with up-to-date information on cyber threats and mitigations for vulnerabilities. If your organization would like to learn more about training opportunities, please contact cssp_training@hq.dhs.gov.

APPENDIX K ICS SECURITY ORGANIZATIONS

Organizations Engaged on ICS Security

The following organizations can advise and assist with ICS vulnerability and risk assessments mostly using their own sets of tools and SMEs. This is merely a subset of a broader community engaged on ICS security.

ICS-CERT http://www.us-cert.gov/control_systems/ics-cert/

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [Dept of Homeland Defense] provides a control system security focus in collaboration with US-CERT to:

- respond to and analyze control systems related incidents,
- conduct vulnerability and malware analysis,
- provide on-site support for incident response and forensic analysis,
- provide situational awareness in the form of actionable intelligence,
- coordinate the responsible disclosure of vulnerabilities/mitigations, and
- share and coordinate vulnerability information and threat analysis through information products and alerts.

AFCESA http://www.afcesa.af.mil/

The Air Force Civil Engineering Support Agency (HQ USAF/A7C) [USAF-centric], CEO Division, provides (on a scheduled basis) specialized ICS and IT teams to apply the ICS PIT C&A Program. AFCESA/CEO's standard procedure is to apply the risk assessment program at Air Force-managed installations on a scheduled basis, with a goal of revisitation every three years; they may visit out-of-cycle on an as-requested basis but will be constrained by already-scheduled assessments. As of this publication, the AFCESA C&A teams operate under authority of SAF/CIO A6, and in accordance with DODI 8500.01E, AFI 33-210, and AFCESA ETL 11-1.

262 NWS http://washingtonairguard.org/194rsw/

The 262d Network Warfare Squadron (262 NWS) is an Air National Guard (ANG) unit operating on Joint Base Lewis-McChord, near Tacoma, Washington. The Washington ANG web site reflects: Nationally recognized as a Cyber Warfare leader, the 262 NWS conducts worldwide network security operations to improve the DOD GiG and the Air Force's network security posture. Recent high-level assessments include the White House Communications Agency, US Central Command, Space Command, and European Command. They also participate in on-going responses to Air Force and DOD cyber incidents, all amidst an increasing number of federal- and state-directed assessments.

NSTB http://www.inl.gov/scada/

To ensure the secure, reliable and efficient distribution of power, the DOE jointly established the National SCADA Test Bed (NSTB) program at INL and SNL. The program works to support industry and government efforts to enhance the cyber security of control systems used throughout the electricity, oil, and gas industries. Among the services available: Control system security product and technology assessments to identify vulnerabilities and corresponding mitigation approaches.

IDART http://idart.sandia.gov/

The Information Design Assurance Red Team (IDART) provides independent, objective, adversary-based assessments of information, communication, and critical infrastructure systems throughout their lifecycle (concept through retirement) in order to identify vulnerabilities and threats, improve design, and assist decision makers with choices in the development, security, and use of their systems. [*Operates out of Sandia National Laboratory*.]

> "The greatest strength of a 21st century grid—evolving technology—may also present opportunities for additional vulnerabilities. Networks of computers, intelligent electronic devices, software, and communication technologies present greater infrastructure protection challenges than those of the traditional infrastructure. Notably, a smarter grid includes more devices and connections that may become avenues for intrusions, error-caused disruptions, malicious attacks, destruction, and other threats."
>
> *A Policy Framework for the 21st Century Grid (p. 49)*

ATTACHMENT 1 MAPPING INTERDEPENDENCIES & ASSESSING RISK

With reference to the eight-step process introduced at the beginning of this handbook, this section will facilitate the following activities:

- **Mission analysis**
- **ID assets**
- **Determine ICS dependencies**
- **Determine ICS connectivity**
- **Assess risk**
- **Prioritize risk management actions**

This leaves the following activities to be addressed by the installation ICS security team.

- **Implement actions**
- **Monitor and reenter the cycle as required**

Roles and Responsibilities

Facilitator

The Installation Commander should appoint a facilitator for this data collection. The results from this effort will assist in determining priorities for resource commitment decisions. The facilitator will have the following responsibilities:

- Authority to gather the required data
- Assembling the experts related to infrastructures that support the missions
- Collating data related to the system dependencies
- Documenting the dependencies of systems, infrastructures, and interconnections (spreadsheet, database, diagrams, etc.)

The duration of this effort depends on the depth of knowledge and documentation of the existing systems. Documenting processes that do not exist, have been abandoned, or were never installed will diminish the value of this. Rigor should be applied to the process of ensuring the dependencies and interconnects are characterized as precisely as possible. This activity also may need to be iterative; a lightning strike knocking out power may expose a connection that was unknown, at which point the diagram/table should be updated as this will alter the relative importance values. The initial amount of time to allocate would be one hour per infrastructure or one-half day for a large meeting with several infrastructures. The facilitated meetings (combined) should not take more than one day for each mission. Additional time can be determined based on the outcome of the first session. Incomplete

groups of data can be collected and documented. Gaps should be noted and filled as experts or data become available.
CAVEAT: Some data may require a clearance to obtain and may result in generating classified documents. A derivative classifier or classification authority should be consulted prior to beginning this effort. The documentation will be, at a minimum, "For Official Use Only."

Some data may not be obtainable. Remember, this is not documenting how the processes work; this is documenting the mission dependencies on processes and systems that in turn depend on one another. Here are examples of utilities and infrastructures that should be part of this effort:

- Electricity
- Fuel
- Water/Waste Water
- Natural Gas
- Security (gates, doors, surveillance, etc.)
    - If security is the mission, then ensure security and the systems/networks security uses are represented in the diagram. If security is a mitigating measure, then make notation of this. Essentially, if the doors lock due to a power outage of the security system, can the mission still function?
- Lights (emergency, runway, search, etc.)
- Emergency Services
- Communications (networks, wired, wireless)
- People (groups, organizations, contractors, etc.)
- Control systems, SCADA systems, HVAC systems, etc.

Subject Matter Experts

The utilities and infrastructures listed above involve people who have expert knowledge about how they connect to other systems or what systems they depend on. They will be supplying the data that builds the diagram/table discussed below. How the system works will sometimes supply additional information on the dependencies and interdependencies.

Example: If the entire water system depends on one electrical feed, then the details of how the water system works will not be as useful as the fact that there is one electrical connection. If the details of the water system identify which HVAC, waste water, potable water, and electrical generation systems depend on the water, then those details are indicating downstream dependencies that need to be documented.

To focus all participants on the objective of this activity, the facilitator may have to make leading statements or ask pointed questions such as:

- "If power were cut, how long can you remain operational?"
- "If the temperature in this building reaches 90 degrees, will the equipment remain functional?"
- "If a <insert disaster> destroyed the <insert part of the building>, would that impact our <insert infrastructure>?"

Using the Diagram

The following figure (Figure Atch1-1) is a representation of a fictitious mission. Each hexagon represents a system or process boundary. The connections between the systems indicate dependencies. The numeric values represent the relative value to one another starting with a base value of 1 for the mission and escalating with each dependency. The rules for escalating the value will be discussed later in this section. Looking at this figure, what system or group of systems has the highest value? Are they inside or outside of the jurisdiction boundary?

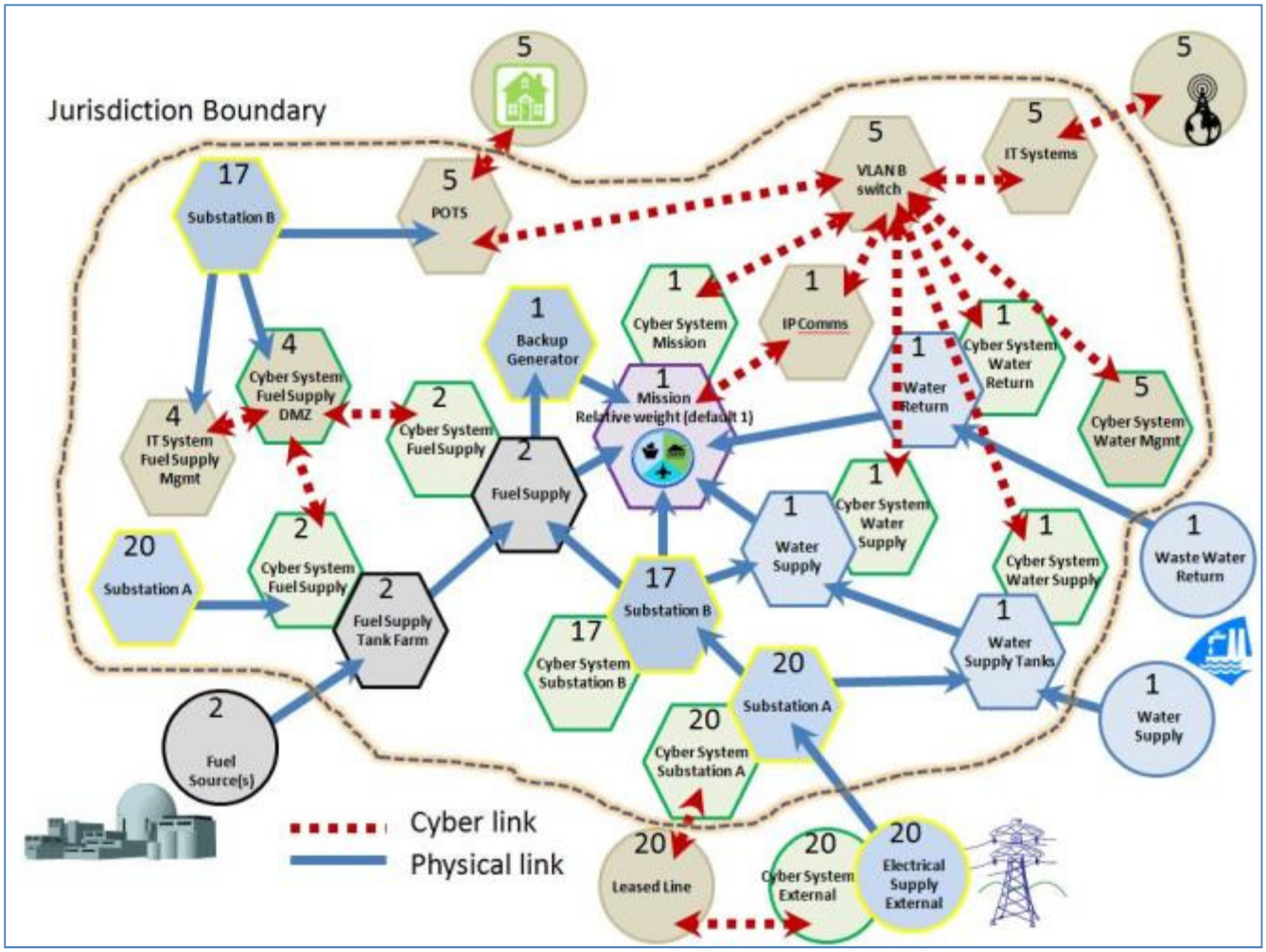


Figure Atch1-1. Example Mission Interdependencies

The figure has color coded hexagons to make finding items easier. For example, electrical systems are blue with a yellow outline. The cyber systems (control systems) associated with the electrical systems are indicated as their own green hexagons. The electrical systems located at the center bottom of the figure have the highest relative importance. The leased line, electrical supply, substation A, and their associated cyber systems (control systems) all have values of 20. The quick meaning is that without electricity, the rest of the systems are likely to be non-functional. The pumps will no longer work to deliver fuel or water to the mission. The IT equipment will no longer be powered. The only item that would remain functional would be the backup generator located to the upper left of the mission (in the middle). This would allow the mission to function at least until the fuel for the backup generator was consumed.

Taking another look at the figure, in the upper-right corner there is a virtual local area network (VLAN) switch with quite a few connections. If there was found a vulnerability that allowed switching from one VLAN to another, could an intruder from the water cyber system get into the process cyber system? That VLAN switch concentrates a significant portion of the cyber traffic around that mission. As such, that component is fairly significant to the successful operation of the mission. The numeric value of 5 indicates the relative importance.

Without prior knowledge of the mission or how the systems operate, a determination can be made of the relative importance of the systems with a quick glance. Another potential representation of this data would be as a topological map imposed on the facility. The highest point would still be the electrical systems. When attempting to control or secure an area that is on low ground surrounded by high ground, are defenses placed on the low ground or the high ground? This diagram and method for generating this diagram should help make that decision, back that decision up with numeric values based on the infrastructure in place, and then apply resources as the installation commander sees fit.

Rules for the Mapping of Interdependencies

The following definitions will be useful:

- ***Missions*** are comprised of ***functions***
- ***Functions*** have requirements in terms of ***utilities***, ***systems***, and ***people***
- ***Utilities***, ***systems***, and ***people*** have requirements as they are supplied by additional layers
- ***Systems/Process*** – An object/component or group of objects/components that accomplish a result
- ***Object / Component*** – An item or group of items that accomplish a task
  - A valve, PLC, temperature indicator, and computer are all components. A system would be the combination of all of them together performing HVAC. A pumping station may comprise of several pumps, controllers, communications, and power components.
  - Sometimes an object or component is a system in and of itself. A managed switch may be necessary to break out as a system boundary because it intersects several networks and segments them with VLANs.

Each layer beyond the initial layer of utilities, systems, and people may comprise a system in and of itself that needs to be identified by the boundaries. Two separated control systems running two segmented parts of a system would be two different representations linked by a process system physical connection. Physical and cyber systems should not be combined so the impacts to one can be seen on the other. The cyber system should be attached and will inherit the value from the process. An example is shown in Figure Atch1-2 below. The SCADA/ICS cyber systems may have several network boundaries they traverse, this is also shown in the figure where the system on Substation A and the system on Electrical Supply External are using a Leased Line to communicate. The Leased Line is owned by a different group and the communications between the two systems depends on it. It is not uncommon to have shared data highways, such as a fiber optic ring, that infrastructure use to communicate. Treat shared interconnects (e.g., a fiber optic ring with the associated switch gear) as a system/process.

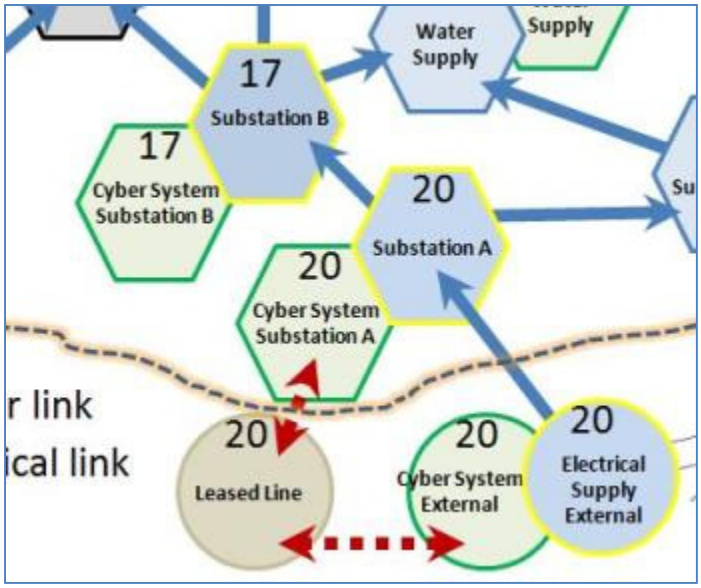


Figure Atch1-2. ICS Representation

Use the following types of diagrams and drawings to assist in creating the interdependency diagram:

- Network diagrams
- Cabinet drawings
- Electrical drawings
- Process diagrams
- Site location diagrams

Use names or locations for tie-in points to components that are connected to multiple components or the diagram may become overly cumbersome. An example of what to do is shown in Figure Atch1-3. The VLANB switch has multiple cyber connections that overlap other systems. While this does represent the connections, this can make the diagram difficult to read.

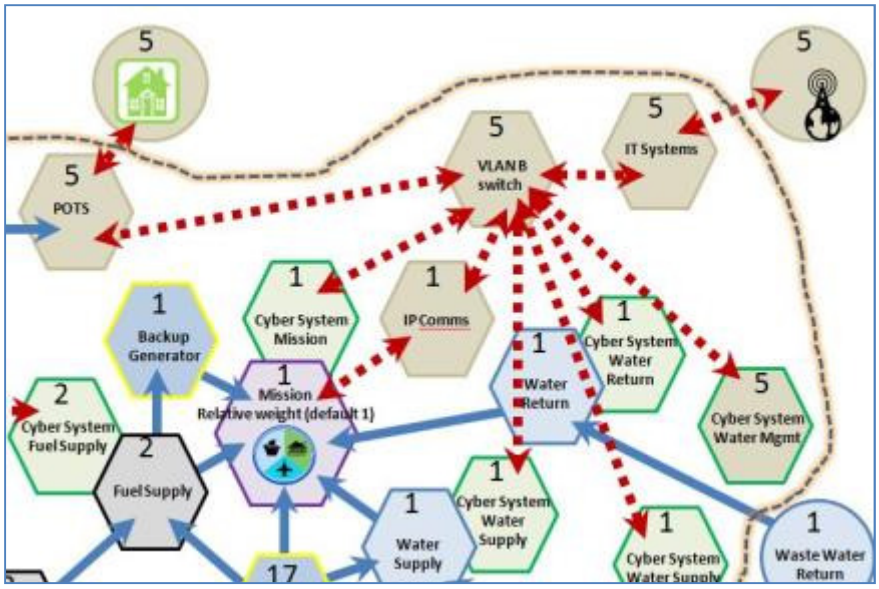


Figure Atch1-3. Congested Dependencies

An alternative way of representing multiple connections is to make an additional object with the same name and make the dependency connections. The difficulty in this solution is in finding the partners. In Figure Atch1-4, both Substation A and Substation B are split in order to keep the diagram cleaner. Network boundaries are also shown in Figure Atch1-4. The cyber systems for the Fuel Supply have a DMZ network with which they both communicate. The DMZ network then has an additional network that it communicates with where the data from the Fuel Supply systems is accessed. A historian passing data to an archive server on an IT network is an example of this type of architecture.

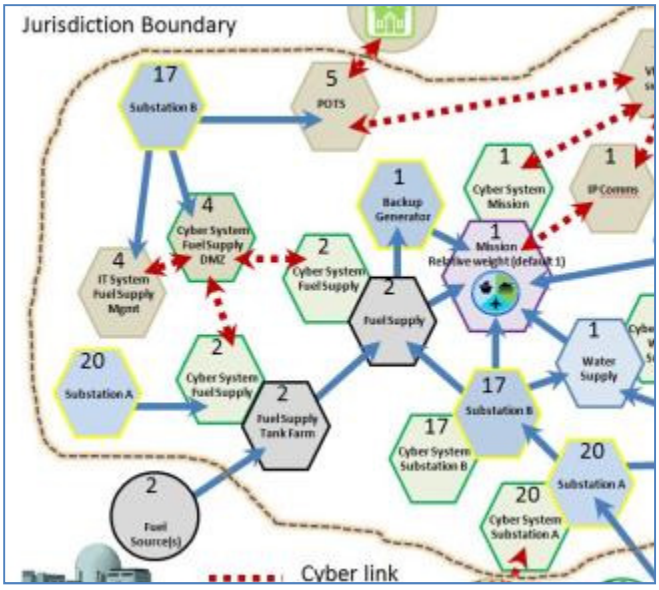


Figure Atch1-4. Decongested Dependencies

The diagram itself should show the dependencies of each system relative to the mission going outward until the installation commander reaches a point where he/she no longer has ownership. At that point, the system dependencies end as indicated by circles in the diagrams above.

The numeric values are assigned to each process or system based on this one rule.

- *A system inherits the values of all of those systems that depend on it.*
  - *The mission value is set to 1.*
  - *All other systems derive their values from the mission value*.
  - *Circular connections are handled consistently (choose to either add them or do not add them)*

The easiest way of generating these values is to use a database or a table in Excel. An example table is shown in Table Atch1-1. Do not generate these values while determining dependencies. Attempting to do so will not benefit the facilitated meeting. The table should contain these columns: *Process/System Boundary, Zi (relative importance), Dependants*, and *geographical information services (GIS) coordinates of the Process/System (optional).*
The cells should be linked as indicated by the cell references depicted. The geographical information services (GIS) data are the GIS coordinates of that component, they are optional. Zi is the aggregated impact or importance value of the component based on dependencies.

Table Atch1-1. Example Relative Importance of Interdependent Systems

	A	B	C	D	E	F	G	H
1	Process / System Boundary	GIS Data	Zi [=sum(D1…Dm)]	D1	D2	D3	D4	D5
2	Mission		1					
3	Cyber System Mission		=SUM(D3:H3)	=C2				
4	Backup Generator		=SUM(D4:H4)	=C2				
5	Fuel Supply		=SUM(D5:H5)	=C2	=C4			
6	Cyber System Fuel Supply		=SUM(D6:H6)	=C5				
7	Cyber System Fuel Supply DMZ		=SUM(D7:H7)	=C6	=C9			
8	IT System Fuel Supply Mgmt		=SUM(D8:H8)	=C7				
9	Cyber System Fuel Supply Tank Farm		=SUM(D9:H9)	=C10				

10	Fuel Supply Tank Farm		=SUM(D10:H10)	=C5				
11	Substation A		=SUM(D11:H11)	=C17	=C12	=C9		
12	Substation B		=SUM(D12:J12)	=C2	=C16	=C5	=C20	=C7
13	Cyber System Substation A		=SUM(D13:H13)	=C11				
14	Cyber System Substation B		=SUM(D14:H14)	=C12				
15	Leased Line		=SUM(D15:H15)	=C13				
16	Water Supply		=SUM(D16:H16)	=C2				
17	Water Supply Tanks		=SUM(D17:H17)	=C16				
18	Electrical Supply External		=SUM(D18:H18)	=C11				
19	Cyber System External Electrical Supply		=SUM(D19:H19)	=C18				

If this were mapped to a GIS map using an alternative elevation of the relative importance, the data would represent terrain that needs securing. The lower elevations are the items of interest and the areas of higher relative importance would be key locations to control the region. The scope of this project prevents the creation of a graphical tool kit so the variations of the graphical depiction will be based on the people contributing to this activity. A white board "exercise" would also work to create a physical image depicting the interdependencies.

Generating the diagram and table

The facilitator should use materials they have at hand. A large white board, poster-sized paper hung on the wall, or poster-sized paper on a tabletop are examples of suitable mediums.

1. Starting with the mission, draw an object and label it "mission" or use the proper mission name.
2. Describe the mission and its functions to the assembled experts and draw radial lines outward from the mission object to show dependencies.

Example: The facilitator makes the statement, "The mission is to provide bombers; which require maintenance, fuel, runways, ordinance, and crew." The facilitator draws radial lines outward connecting it to objects labeled "maintenance," "fuel,." "runways," "ordinance," and "crew."

3. The experts assembled should represent people knowledgeable about each function with which the mission relies. Some experts will know about several functions. In an

orderly fashion, capture everyone's input. Drawing objects and connecting lines to show the systems/processes and dependencies. Use arrows if the dependency is one way with the arrow pointing toward the downstream or consumer component. Resolve conflicts in a professional manner. Resolution may take the form of a field trip, a field test, or a discussion. If the resolution must be postponed until after the facilitated session, document the object with a question mark to show uncertainty.

NOTE: Computer networks should be viewed in a frame of consumer/publisher. What system produces the information and what system consumes the information. The consumer is dependent on the producer. The producer is not dependent on the consumer.

4. Document the diagram. This can be done by printing, photographing, or whatever means is suitable for the medium.
5. Generate a table of Relative Importance of Interdependent Systems based on the diagram.
6. The table will generate values for each system/process based on the documented dependencies.

Assessing the risk and prioritizing risk management actions

Assessing the risk and prioritizing the risk management actions on a macro scale requires a high-level determination of cyber risk. The purpose of the high-level determination is to prioritize areas of focus to perform more time consuming assessments. Performing this calculation will take into account how a system is used or monitored.

Calculation of Priority based on Use

Maintenance for mechanical devices is fairly well understood. There are differences in opinions on how best to perform maintenance. Cyber systems require a different kind of maintenance. The concern is the chance that, due to a lack of information technology maintenance, the control system will be an easier target for hacking. A quick search using the NIST National Vulnerability Database (http://nvd.nist.gov/view/vuln/search) is presented in Table Atch1-2. These are the rates of reporting, not necessarily the rate of discovery. Each product has the vulnerabilities it was created with; products do not create new vulnerabilities by existing. As interest in a system increases, the number of reported vulnerabilities increases. This is different from a mechanical device that wears out over time. Programs do not wear out, though the vendor may discontinue the product.

Table Atch1-2. Number of Reported Vulnerabilities

Company	Reported over 3 months	Reported over 3 years	Avg / Month
Oracle	185	984	27.3
Microsoft	83	876	24.3
Linux	121	855	23.8
Adobe	29	535	14.9
McAfee	1	25	0.7
Symantec	20	98	2.7
Invensys	7	14	0.4
ABB	6	47	1.3
Siemens	9	34	0.9
Cisco	56	473	13.1
Juniper	0	16	0.4
Dlink	1	10	0.3
Intel	11	138	3.8
AMD	2	9	0.3
NVIDIA	3	7	0.2
ATI	7	68	1.9
Dell	1	13	0.4

Access to a control system allows users to perform actions. Stuxnet showed how important this is. The vulnerabilities used by Stuxnet were not vulnerabilities in the Siemens software; they were vulnerabilities in the operating system. Once on the consoles, Stuxnet made use of the Siemens software to perform tasks it was designed to do. Any vulnerability that allows arbitrary execution of code can allow malicious software access to control system functions that are available to the user account the vulnerable program is using.

A control system uses three methods of user access control:

1. The first is no security. The software will run as the operating system account currently logged in. These types of systems often run as an administrative level user. If one can log into the console, one can perform any action on the system such as opening breakers or valves, adjusting set points, or downloading new configuration to the field controllers.
2. The second method is a custom user account manager on top of the operating system accounts. This method can result in security being turned on/off for the control system and circumstances where no user accounts exist for the control system thereby locking the console until it is rebuilt with an image or reinstalled. This method will typically use an auto-login account for the operating system and then have the operations personnel use their own custom user account to gain access to the control system interfaces. The auto-login account is often an administrative level user.
3. The third method is to use accounts integrated into the operating system user accounts. This is more common of systems designed after 2001. This will be a mix of user accounts with role-based privileges. A look at the processes running on the console will show a number of user accounts that are control-system specific that likely have administrative rights, which are used to keep key system functions operational.

This is why software management and system monitoring is important for control systems. Assume that the system can be compromised then watch the system for aberrant behavior indicating unstable code. Achieving this level of monitoring takes resources in the form of people, procedures, and technology. All of which cost money to deploy and maintain. In the previous section, the interdependencies of the infrastructure were determined and a table was built. The relative importance to the mission was determined for each system. That value does not take into consideration operational conditions or mitigation measures in place. The following columns should be added to the table of relative importance:

- Maintenance (patching, evaluating/testing patches, etc.) performed regularly for
  - Operating system
  - Hardware
  - Third-party software
  - Control system software
  - Customized software
- System monitoring frequency (how often is the system used/observed)
- System log (all logs) monitoring frequency
- Physical connections

The resulting table with values is shown in Table Atch1-3.

Table Atch1-3. Operational Considerations for Relative Importance

	A	I	J	K	L	M	N	O	P
1	Process / System Boundary	Operating System	Hardware	Third-Party Software	Control System	Customized Software	Monitoring Frequency	Log Monitoring Frequency	Connections
2	Mission								
3	Cyber System Mission	1	0	0	1	1	0.2	1	1
4	Backup Generator								
5	Fuel Supply								
6	Cyber System Fuel Supply	1	1	1	1	1	0.1	1	2
7	Cyber System Fuel Supply DMZ	0	1	1	0	1	0.4	1	2

Operating System	Value of 1 if this needs attention. Value of 0 if this is maintained and fully patched.
Hardware	Value of 1 if this needs attention. Value of 0 if this is maintained and fully patched.
Third-Party Software	Value of 1 if this needs attention. Value of 0 if this is maintained and fully patched.
Control System	Value of 1 if this needs attention. Value of 0 if this is maintained and fully patched.
Customized Software	Value of 1 if this needs attention. Value of 0 if this is maintained and fully patched.
Monitoring Frequency	Value based on the frequency of operations monitoring - Continuous: 0.1, Hourly: 0.2, Daily: 0.4, Weekly: 0.8, Monthly: 1.0, Yearly: 2.0, More: 4.0
Log Monitoring Frequency	Value based on the frequency of monitoring any logs - Continuous: 0.1, Hourly: 0.2, Daily: 0.4, Weekly: 0.8, Monthly: 1.0, Yearly: 2.0, More: 4.0
Connections	Number of interfaces. Console +1, Network (wired / wireless) +1, USB/Serial/Firewire/CDROM/DVD etc. +1 (max 3)

The calculation for the relative importance of interdependent systems (Zi) was the sum of the value of the dependencies shown as the yellow highlighted cell, C3 of Table Atch1-4.

Table Atch1-4. Subset of the Example Relative Importance of Interdependent Systems

	A	B	C	D	E	F	G	H
1	Process / System Boundary	GIS Data	Zi [=sum(D1…Dm)]	D1	D2	D3	D4	D5
2	Mission		1					
3	Cyber System Mission		=SUM(D3:H3)	=C2				

The table additions of columns I through P will be used in the calculation of the relative importance to mission modified by operational considerations. This value will be called the *Cyber Readiness*. Attention should be given to the entries with higher values.

An additional column should be added to the table so the calculations can be automated. For the purposes of this calculation, row 3 in the table will be used. All cells will be using this reference. C3 represents Zi.

Cyber Readiness
= Log10(C3) * sum(I3:M3) * N3 * O3 * P3

These values are then the risk prioritizations of the ICS/cyber components that support the functions with which missions rely. The higher values represent more at risk to the system. Some systems will have mitigations already in place, having the conversation with the system owner can determine if this is the case. The judgment of what resources to place should never be solely on the numeric value, however the numeric value can assist in making that determination.

ATTACHMENT 2 CHECKLIST OF RECOMMENDED ACTIONS

The following tabular format checklist presents recommendations made earlier in the handbook using a modified DOTMLPF-F[37] construct. The checklist does not cover every last action that may be taken to secure installation ICS. Additional actions may be identified during assessment or even in the midst of implementation. Also, this is generic, meaning that applicability is broad rather than specific. Each installation will have differences, in some cases significant, in control systems architectures, security measures already in place, organizational and personnel management, and missions. The "one-size-fits-all" approach offered here will indeed yield a more secure ICS, but a closer fit will require tailoring (such as using other tools, requesting assistance of SMEs, etc.).

Actions are not listed in a particular order, except that policy should first be well-established so as to facilitate implementing actions in other areas. Nor do actions need to be implemented sequentially; many actions may be undertaken in parallel.

NOTE: A separate table may be used for each type of ICS or by mission supported.

The columns in the table are:

- FOCUS: **C**OTMLPF-P area
- ACTION: ICS security action to implement
- COMMENTS: Notes/comments about that action
- PRI #: Priority assigned to the action (self-defined priority scheme and criteria)
- POC: Person or office with primary responsibility for managing that action
- ASSGND: Date assigned by installation commander or ICS security team
- DONE: Date completed

Blank rows are included at the end of each "Focus" section for installation-specific additions.

[37] Modified by replacing the "D" with a "C" for cybersecurity.

TITLE <*name of control system, infrastructure, or mission*>

MISSION(S) SUPPORTED:

OTHER INFORMATION:

FOCUS	ACTION	COMMENTS	PRI #	POC	DATE ASSGND	DATE DONE
	POLICY					
P	**Review ICS policy requirements with ICS Security Team** **Review existing policy(ies) and amend/adopt as appropriate** **Develop policy for the following:** • Roles & responsibilities (including vendors & third parties) • Vulnerability & risk assessments • Access control • Security of assets • Configuration control • Acquisition of hardware &					

O L I C Y	software • Patch management • Inventory accounting • Education, training & exercises	
	Review ICS service level agreements with vendors and integrators	Changes to ICS systems often require vendor and/or integrator approval or support, which may not be covered in existing service level agreements
	Set software and SDLC requirement standards for ICS procurements	See the DHS Cyber Security Procurement Language for Control Systems document, http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf
	Create incident response management plan with vendor, integrator, or third party ICS provider	Incident management across business boundaries, i.e. incident coordination with commercial energy providers, requires significant planning and cooperation; better to have the plan worked out before an incident occurs

	LEADERSHIP	
	Promulgate policies	
	Schedule awareness briefings for ICS managers, operators, & users	
	Attend stakeholder events	Gain and enhance situational awareness
	Collaborate with ICS vendors and service providers	Focus should be on security and training
L **E** **A**	**Develop new or adapt existing plans to address ICS. Plans include at least:** • Disaster Recovery • System Security • Contingency (include response	

D	to INFOCON, FPCON)	
E	• Continuity of Operations	
R	**Add key ICS information to the Commander's Critical Information List**	Think of most if not all ICS-related information as at least FOUO
S		
H		
I		
P		

PERSONNEL

	Train all ICS managers, operators & users	Include policies, roles, security, incident response handling, etc.
	Develop a refresher training program	
	Perform background checks on everyone with ICS responsibility	
	Require confidentiality or non-disclosure agreements	

P	**Create an ICS incident response team**	Can model on existing IT CERT or on DHS's ICS-CERT
E	**Enforce system access controls**	Includes network (logons) and physical (cipher-locked doors)
R		
S	**Maintain rosters for access to physical facilities**	
O	**Immediately delete all access (physical and system) of those who resign, retire, move, are fired, etc.**	This must include third-party vendors, contractors, etc. as well as direct employees and military
N	**Provide checklists/SOPs to each operator position as appropriate**	Can be used also for training
N		
E		
L		

TRAINING

	Ensure ICS-specific training prior to granting individuals access	
	Require IA training (initial & refresher)	In some cases, users of IT components of ICS

T R A I N I N G	**for all ICS managers, operators & users**	are overlooked in IA training
	Provide threat & vulnerability awareness via appropriate venues	
	Document all training; maintain currency	
	Exercise ICS-related plans	
	Include ICS in base-level exercises	For example, when INFOCONs are implemented or when FPCON is elevated
ORGANIZATION		
O R	**Appoint an ICS IAM**	Most installations with DOD networks already have an assigned IT network IAM; an ICS IAM is distinctly separate and trained specifically to ICS issues (but will coordinate with IT IAM)
	Assign responsibility for ICS configuration control	
	Specify ICS roles & responsibilities of	

G A N I Z A T I O N	**at least:** • Commander • CEs/PWs • Communications/IT • Operations	
	Identify leads for developing ICS-specific plans	Or for incorporating ICS considerations into existing plans
	Publish chain-of-command for incident response	
	Identify roles & responsibilities of vendors, third parties	
	FACILITIES	
	Create a map/chart/topology of all physical facilities	Include buildings, rooms, panels, cabling, etc.

FACILITIES	**Identify & inspect all physical facilities**	
	Develop a plan of action & milestones for correcting facility security deficiencies or weaknesses	
	Identify and secure portable assets	For example, fly-away kits, laptops, spares. Depict their locations on the facility map
	Secure all cable terminations (their housings)	Wiring termination boxes often are located in isolated areas and with only minimum security controls (e.g., easily cut padlock, wire with lead breakage seal)
MATERIEL		
M	**Document the entire ICS infrastructure**	Include logic diagrams, data flows, dependencies, and particularly connection to mission/mission support assets
	Assign responsibility for accountability for physical assets	Include acquisition, configuration, inventory, etc.

A	**Establish acquisition policy and process**	
T	**Require testing of any new component or program off-line**	Always test before adding to the live infrastructure
E	**Identify and control all ICS documentation and software media**	
R	**Ensure all replaced components are "cleaned" prior to disposition**	
I	**Provide failover or redundant servers and other components serving critical mission functions**	
E		
L		

CYBER SECURITY

	Define & defend perimeters; approaches may include: • Segmentation • DMZs	Part of a comprehensive defense-in-depth strategy

C Y B E R S E C U R I T Y	• Enclaves	
	• VPNs to cross defended boundaries when necessary	
	Control individual access:	
	• Assign individual/unique logon IDs and passwords	Follow standard DOD practices
	• Design user access control architecture based on Least-User Access (LUA) model	
	• Require role-based access control (RBAC)	For existing as well as new accounts
	• Disable all “guest” or anonymous accounts	
	• Set UAC policy for event log auditing	ICS systems and applications are relatively static; any change to UAC configuration at the operating system, application, and data levels need to be identified immediately and reviewed for security implications
	• Set timeline and threshold monitoring requirements for UAC events	Event logs (functional and security) need to be reviewed in a timely manner; it will not do the teams any good if an IT IDS team reviews the alerts because the IDS team will not understand ICS traffic initially
	• Ensure functional UAC auditing and monitoring thresholds are	Security-impacting changes to an ICS are more likely to be detected through functional

	put in place	incident evaluation rather than through security event monitoring; make sure ICS admins are reviewing their systems for security-impacting events
	• Ensure audit configuration and log monitoring on ICS systems can detect unusual egress traffic from privileged user accounts	As with previous comments, egress traffic from the ICS networks to the corporate/military or Internet need to be evaluated so a baseline of normal egress traffic can be established; unusual or anomalous egress traffic from privileged accounts needs to be identified and evaluated as quickly as possible
	Protect operating system:	
	• Disable all unnecessary network services	
	• Use (and keep current) virus-checking software	Virus detection programs may be difficult to update on live systems, and therefore will require diligence in maintaining currency
	• Establish software lifecycle management policy	Out-of-date software of any sort (firmware, operating system, third party/COTS, custom code, development frameworks, etc.) should all be maintained and within n or n-1 releases of a vendor's supported software
	• Enable audit logging & monitor	
	• Remove all unnecessary programs	

C Y B E R

S E C U R I T Y	• Implement security policies per vendor best security practices list	Security configurations should be done on each OS in addition to the external access controls like port configuration; this means disabling autorun, limiting remote registry access, etc.
	• Consider using IDS	If consider, do so judiciously and in close consultation with cybersecurity specialists who probably already had implemented an IDS on the IT network. Many IDS marketed specifically for ICS may not actually add more value to defense than already provided by the IT side IDS.
	Protect data:	
	• Encrypt data in motion (at least on the IT side)	Probably not able to encrypt data on the purely ICS component side, such as between a PLC and a master server; definitely unable to encrypt between a PLC and a sensor
	• Enforce controlled access to stationary data (files, databases, etc.)	
	• Back up system routinely and keep backups secure & accessible	A backup held exclusively by a vendor will not be "accessible" in certain circumstances, such as a FPCON Charlie or Delta
	• Implement separate data management procedures for business/ICS/operational data and data configuration files	Data segregation provides another security layer and helps prevent random failures of the OS/application from impacting data; since config files are often transferred from failing

		systems to the new system without being checked, malware authors hide RAT software in them
	• Map the flows of critical data at least annually to ensure data is being protected and accessed appropriately	Identify and map exactly where critical data goes throughout its usable life cycle to ensure you know exactly where it can be accessed and what protections are in place; use a data flow diagram and threat modeling tools to ensure appropriate trust boundaries and technical security controls are in place
	Control web services and Internet access:	
	• Disable unnecessary web services	
	• Use “white”/”black” lists	Whitelisting typically is favored over blacklisting; situational determination required
	• Enforce acceptable-use policy on Internet access and browsing	
	• Use a web application firewall (WAF) if possible	Put a WAF in between the ICS network and other networks to ensure known attacks can be blocked before they hit vulnerable endpoints. In most cases, adequate web content and service filtering cannot be adequately performed at the host level on an ICS network server or endpoint; the static

C Y B E R

S E C U R I T Y		nature of ICS networks make the WAF easier to implement
	• Implement best security practices per browser vendor	OS security is not sufficient to defend against endpoint attacks over port 80; browser level security controls need to be put in place as well
	• Use native browser tools and third party browser security applications	Use of tools like NoScript or BetterPrivacy prevent automatic execution of scripts within the browser and prevent auto-execution of malware via browser components or web services
	• Develop and implement web component and services software development lifecycle	Web service and web component attacks against the browser are a big deal; browser plug-ins, extensions, and services must be controlled to prevent attack methodologies such as JIT spraying, ROP, etc.
	• Perform web app security scans before and after web services are enabled on servers and hosts	Use of web-based services presents a significant attack surface on servers and hosts; ensure a baseline of those services has been performed so any security gaps can be identified
	• Incorporate web app security touchpoints into the standard development lifecycle of all web-enabled software	Make sure vendors, integrators, and in-house development teams are testing their web apps and have a mature software security development program for any software deployed on a system
	• Configure systems to deny	Keep malware from hooking into systems or

C Y B E R S E C U	long-term storage of web service information like cookies and temporary cache	gaining access via long term cookie and data storage by web services
	Identify and manage all network communication access points; disable those not needed and protect all others • Modems/dial-up • Wireless • Cable/DSL • Fiber-optic • Satellite • Ethernet • Cellular	
	Identify and manage all removable media access points; disable those not needed and protect all others • Mobile devices (cell phones, MP3 players) Removable hard drive storage devices (SAN disks, USB thumb drives, flash drives)	

R

I

T

Y

Identify and manage all messaging service access points; disable those not needed and protect all others

- SMS/MMS text messaging
- VoIP
- Instant messaging
- Unified communications solutions
- Intranet server resources (SMB messenger service, remote registry, etc.)

Identify and manage all remote management applications, services, or functions, disable those not needed and protect all others

- Web management interfaces

Web management interfaces exist for systems from the firmware on up to the data layer of the OSI model; every one of them need to be identified and secured

- Remote hardware management tools
- Asset management and configuration software
- Host-based security software (AV, HIPS, back up services,

CYBER SECURITY

etc.)

Ensure there are no "hidden" or "backdoor" access capabilities

Y

C

Y

B

E

R

S

E

C

U

R

I

T

Y

ATTACHMENT 3 COMMITTEE ON NATIONAL SECURITY SYSTEMS INSTRUCTION 1253 ICS OVERLAY VERSION 1

BACKGROUND

The CNSSI 1253 ICS Overlay Version 1 was developed by a Technical Working Group (TWG) charted by the Installations and Environment, Business Enterprise Integration office in 2012. The TWG was comprised of Subject Matter Experts from DoD, DHS, and NIST and the JTANICS staff. The overlay was published in January 2013 and incorporated into the DHS CSET 5.1 tool, released in June 2013.

The intent of the overlay was to bridge the gap between the need to have a standardized process across the DoD to address the growing concern about the lack of ICS cybersecuriity and have basic "primer" that the engineering, information technology, and information assurance community could use in preparation for the DoD issuance of the new DoDI 8500 Cybersecurity instruction and adoption of the NIST Risk Management Framework. The RMF is replacing the Defense Information Assurance Certification and Accreditation Process (DIACAP).

At the same time the CNSSI ICS Overlay was being developed, NIST was also updating the NIST SP 800-53 Rev 3 Recommended Security Controls For Federal Information Systems and Organizations, and the NIST 800-82 Industrial Control Systems Security Guide. As part of the update process, NIST moved the NIST SP 800-53 Rev 3 Appendix I Industrial Control Systems Security Controls, Enhancements, and Supplemental Guidance to the NIST 800-82 Rev 1 Appendix G. This kept the ICS guidance and controls in one contiguous document. NIST is in the process of updating the NIST SP 800-82 to incorporate the new controls developed in the NSIT SP 800-53 Rev 4, with a target date of a spring 2014 release.

The NIST SP 800-82 writers group has incorporated a great deal of the CNSII 1253 Overlay Version 1 content into the draft NIST 800-82 Rev 2, and has created a master ICS Overlay template that can be used by any organization.

Future versions of the CNSSI 1253 ICS Overlay may simply refer to the NIST SP 800-82 Rev 2 or will be a very condensed version of this overlay.

Committee on National Security Systems Instruction (CNSSI) No. 1253

SECURITY CONTROL OVERLAYS FOR INDUSTRIAL CONTROL SYSTEMS

Version 1

January 2013

This Draft version of the Overlay is for informational and instructional purposes only and meant to be used a companion to the DHS Cybersecurity Evaluation Tool (CSET). The Draft version is based on the NIST SP 800-53 Rev 3 publication. The Final version is being revised to follow the new format of the NIST SP 800-53 Rev 4 publication.

Forward

The National Institute of Standards and Technology (NIST) created NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," to establish a standardized set of information security controls for use within the United States (U.S.) Federal Government. As part of the Joint Task Force Transformation Initiative Working Group, the Committee on National Security Systems (CNSS) has worked with representatives from the Civil, Defense, and Intelligence Communities to produce a unified information security framework and to ensure NIST SP 800-53 contains security controls to meet the requirements of National Security Systems (NSS).

Security control overlays are specifications of security controls and supporting guidance used to complement the security control baselines and parameter values in CNSSI No. 1253 and to complement the supplemental guidance in NIST SP 800-53. Organizations select and apply security control overlays by using the guidance in each of the standardized, approved and CNSS-published overlays.

An overlay is a specification of security controls and supporting guidance used to complement the security control baselines and parameter values in CNSSI No. 1253 and to complement the supplemental guidance in NIST SP 800-53. An overlay's specifications may be more stringent or less stringent than the controls and guidance complemented. Overlays may be applied to reflect the needs of different information types (e.g., personally identifiable information [PII], financial, or highly sensitive types of intelligence); system functionality needs (e.g., stand-alone systems, cross domain solutions, or controlled interface systems); or environmental or operationally-driven needs (e.g., tactical, space-based, or test environment).

1. Characteristics and Assumptions

The Industrial Control Systems (ICS) Overlay applies to Platform IT (PIT) systems. As stated in DoDD 8500.01 Cybersecurity Directive, Enclosure 3, "Examples of platforms that may include PIT are:

> "weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems to include supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks)."

ICSs are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs range from non-critical systems, such as those used for building environmental controls (HVAC, lighting), to critical systems such as the electrical power grid.

Within the controls systems industry, ICS systems are often referred to as Operational Technology (OT) systems. Historically, the majority of OT systems were proprietary, analog, vendor supported, and were not internet protocol (IP) enabled. Systems key components, such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Physical Access Control Systems (PACs), Intrusion Detection Systems (IDSs), closed circuit television (CCTV), fire alarm systems, and utility meters are now becoming digital and IP enabled. OT systems use Human Machine Interfaces (HMIs) to monitor the processes, versus Graphical User Interfaces for IT systems, and most current ICS systems and subsystems are now a combination of Operational Technologies (OT) and Information Technologies (IT).

An emerging concept in technology is to refer to the hybrid OT and IT ICS systems as cyber-physical systems (CPS). As defined by the National Science Foundation:

> "cyber-physical systems are engineered systems that are built from and depend upon the synergy of computational and physical components. Emerging CPSs will be coordinated, distributed, and connected, and must be robust and responsive. The CPS of tomorrow will need to far exceed the systems of today in capability, adaptability, resiliency, safety, security, and usability. Examples of the many CPS application areas include the smart

electric grid, smart transportation, smart buildings, smart medical technologies, next-generation air traffic management, and advanced manufacturing."

As these new technologies are developed and implemented, this Overlay will be updated to reflect advances in related terminology and capabilities. This Overlay focuses on the current generation technologies already in the field, and the known technologies likely to remain in inventory for at least the next ten years.

Figure 1 is a typical electrical supervisory control and data acquisition (SCADA) type system which shows the HMI at the operators console, the transmission system infrastructure, and the RTU in the field. At the substation and building level, the meters are monitored in a local Energy Operations Center (EOC) or Regional Operations Center (ROC), which use real time analytics software to manage the energy loads and building control systems, down to the sensor or actuator device level.

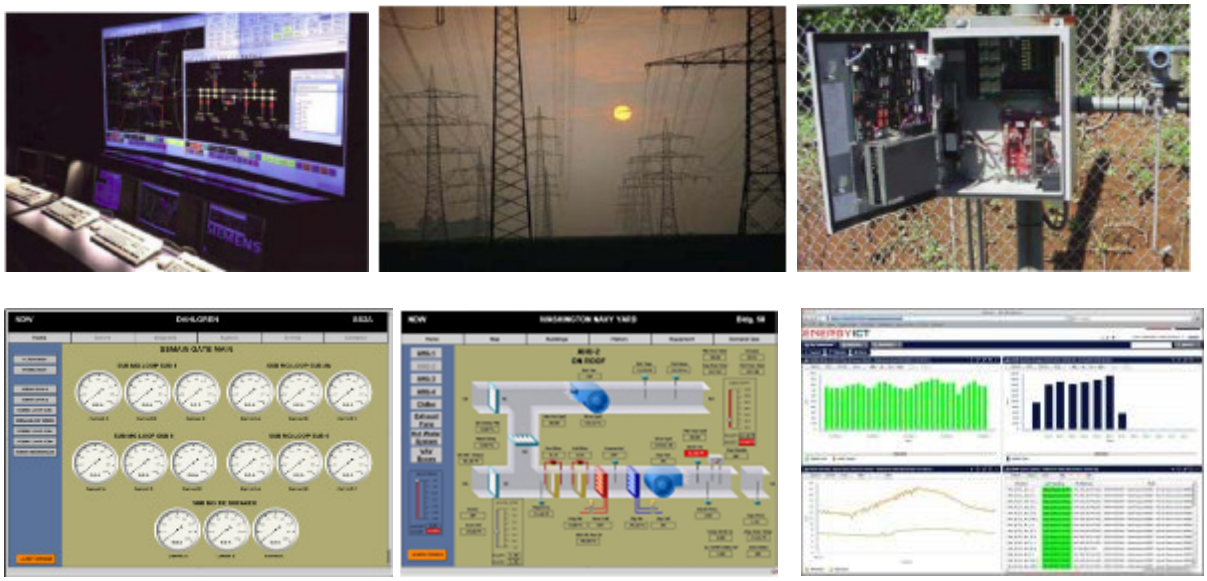


Figure 1 – ICS Human Machine Interface, System, Remote Terminal Unit[38]

ICSs differ significantly from traditional administrative, mission support and scientific data processing information systems, and use specialized software, hardware and protocols. ICS systems are often integrated with mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities. The "front end" portions of these ICSs resemble traditional information systems in that they use the same commercially available hardware and software components. While the majority of an ICS system still does not resemble a traditional information system (IS), the integration of the ICS's "front end" with IS introduces some of the same vulnerabilities that exist in current networked information systems.
ICSs can have long life spans (in excess of 20 years) and be comprised of technology that in accordance with Moore's law suffers rapid obsolescence. This introduces two issues: first,

[38] The pictures and devices shown in this Overlay are for illustrative purposes only and are intended to show typical field devices that are the core elements of OT. This Overlay document does not endorse any specific vendor or product.

depending upon the relative age and isolation of the system, there may not be a patch or upgrade path for components of the system, and second, attempting to patch the component or employing modern scanning methods might disrupt the system. ICSs have experienced complete system shutdown when an intrusion detection system (IDS) or host-based scanning system (HBSS) scan is performed on an otherwise operational ICS. For an ICS, updates should be delayed until after a thorough analysis of deployment impact has been completed. This might stretch out security update timeliness and require flexibility in security control compliance measurement and enforcement.

While many Information Assurance (IA) controls from the baselines can be applied to an ICS, how they are implemented varies, primarily because of technical and operational constraints and differences in the evaluation of risk between ICSs and standard ISs. Interconnections between ICSs and the organizational network and business systems expose ICSs to exploits and vulnerabilities, and any attempts to address these exploits and vulnerabilities must consider the constraints and requirements of the ICS. These constraints can be both technical - most ICS components have limited storage and processing capacity – or practical, as most ICSs are funding and personnel constrained so resources allocated to IA are removed from other functions (such as maintenance), which often adversely impacts the function of the ICS. Unlike most ISs, ICSs are driven primarily by availability, which requires a different approach to making IA decisions.

A comparison of IT versus OT systems is provided in the table below:

Table 1: IT vs. OT Systems Comparison

	Information Technology	Operational Technology
Purpose	Process transactions, provide information	Control or monitor physical processes and equipment
Architecture	Enterprise wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (custom)
Interfaces	GUI, Web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
Ownership	CIO and computer grads, finance and admin. depts.	Engineers, technicians, operators and managers
Connectivity	Corporate network, IP-based	Control networks, hard wired twisted pair and IP-based
Role	Supports people	Controls machines

A significant change in DoDD 8500.01 Cybersecurity Directive, Enclosure 3, is to eliminate the use of the term Platform IT Interconnection (PITI), and adopt Integration and Interoperability:

> "All interconnections of DoD IT will be managed to minimize shared risk by ensuring that the security posture of one system is not undermined by vulnerabilities of interconnected systems.
>
> Interconnections between PIT systems and DoD ISs must be protected either by implementation of security controls on the PIT system or the DoD IS."

In this Overlay, the terms IT and OT are used to define the Tiers Architecture and delineate the boundary between the PIT and DoD IS.

Implementing security controls in ICS environments should take advantage of the concept of common security controls in order to mitigate the constraints caused by the characteristics of those environments. By centrally managing and documenting the development, implementation, assessment, authorization, and monitoring of common controls and security services, organizations can decrease the resources associated with implementing security controls for individual systems without sacrificing the protections provided by those controls, and security controls are then implemented as part of a greater security environment. For example, a control implemented within a service provided by an EOC may be inherited by a system on a mobile platform (i.e. field power generation). Networked systems can, and will, depend on one another for security protections or services as part of a defense in depth strategy. Controls meant to be common across connected systems – access controls, for example – can be provided once and inherited across many, assuming the implementation is adequate to support multiple systems. Every implementation of common controls requires analysis from a risk management perspective, with careful communication among representatives from all interconnected systems and organizations. The new Advanced Meter Infrastructure shown in Figure 2 is being installed on Department of Defense (DoD) buildings, and highlights the challenges and complexities of the new hybrid OT systems. Unfortunately, due to the issues associated with implementing IA for older ICSs, many older (legacy) ICSs will operate in isolation and may be unable to make use of many of the common controls.

Figure 2 – Advanced Meter Infrastructure (Smart Meters) for Electric, Water, Gas

Figure 3 provides a schematic architecture and definition of tiers for ICSs that follows the ANSI/ISA process, but includes additional components/tiers not shown in the ISA architecture.

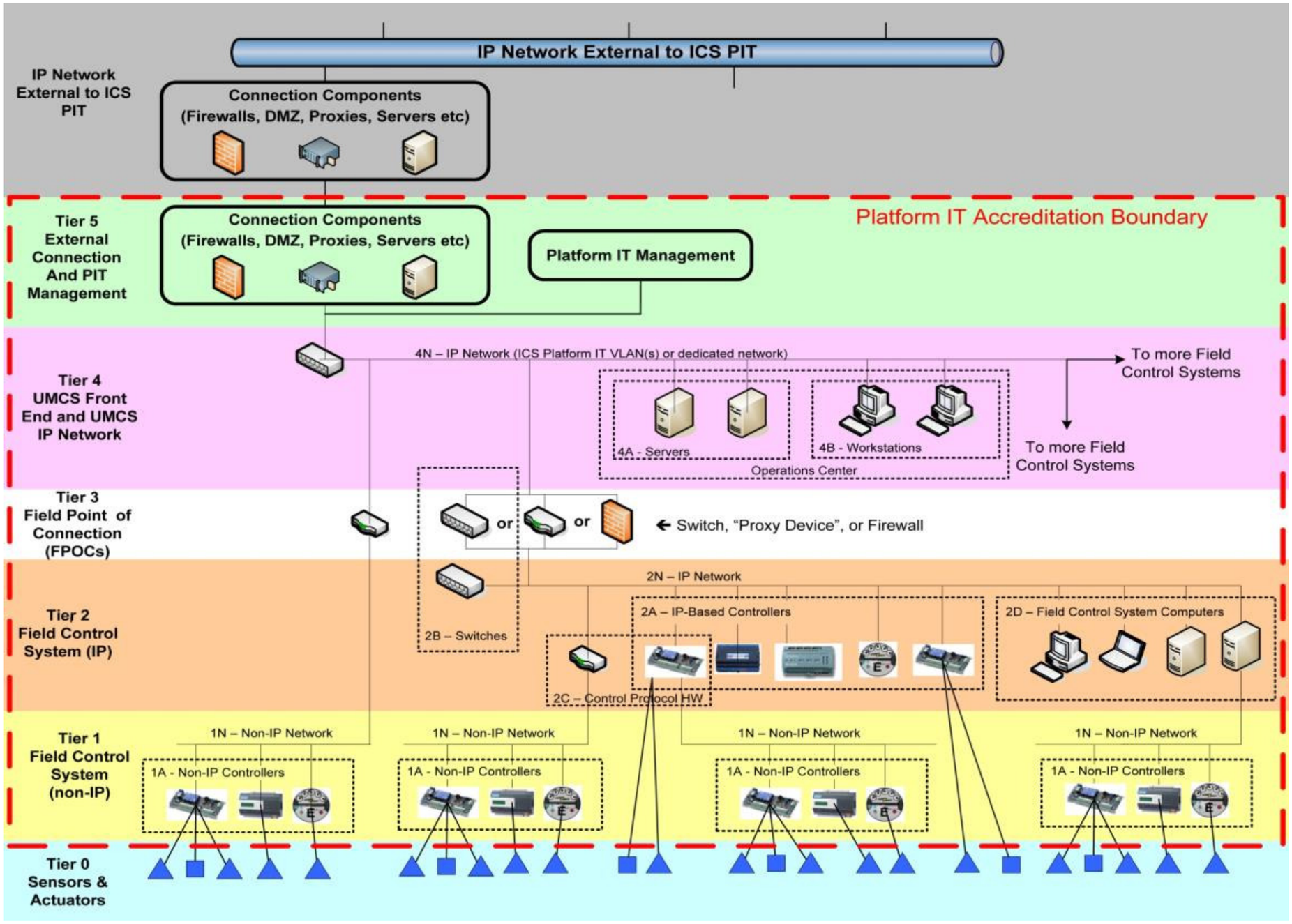


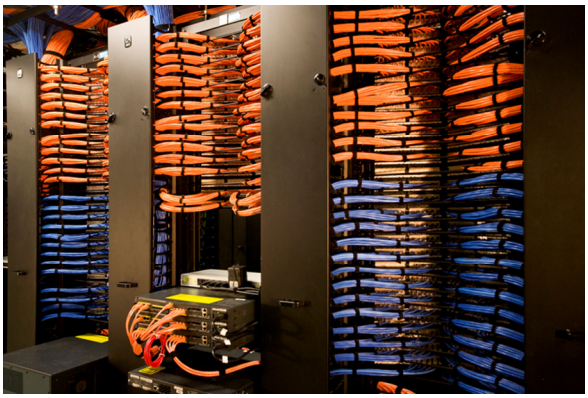
Figure 3 – ICS Tiers

The ICS tier architecture is used to define the accrediation boundary for OT systems and is a logical representation of the OT network. The actual physical system can span many miles; for example, locks and dams, pipelines, electric transmission and distribution systems can have many non-contiguous components, and there are a number of protocols commonly used by ICSs to allow the devices within the tiers to communicate both horizontally and vertically. Some of these protocols are:

- LonWorks
- BACnet
- Modbus
- DNP 3

Illustrations of the components and devices that utilize these protocols are:

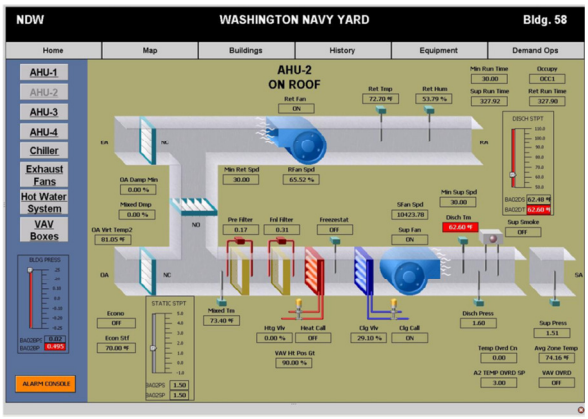
5: A Tier 5 Demarcation Point or Main Point of Presence where the external meets the internal interface.



5: A Tier 5 IT rack and servers located in an Installation Processing Node.
.

Figure 4 - Tier 5: "External" Connection and PIT Management

4-A: A Tier 4 OT rack and servers located in an Energy Operations Center, Special Purpose Processing Node.



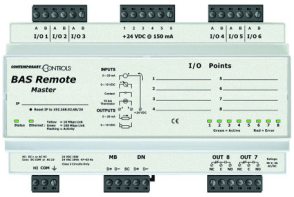
4-B: Workstation or wall display of HMI for the UMCS.

Figure 5 - Tier 4: UMCS Front End and IP Network

3-FS: A Tier 3 FPOC gateway (application layer proxy). The Tier 4 network is Modbus over IP over 10/100 Mbps Ethernet. The Tier 1 network is proprietary over proprietary 2-wire media. Note this is the same device as in 2C-FS.

3-LIP: A Tier 3 FPOC router between 3 LonTalk networks: Tier 1 Lon over TP/FT-10, Tier 1 Lon over TP/FT-10, and Tier 4 Lon over IP over Ethernet.

Figure 6 – Tier 3: Facility Points of Connection (FPOCs)



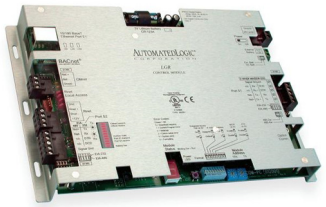
2A-CC: Very basic Tier 2A controller capable of monitoring six analog inputs and reporting their values to the network and setting two outputs. Network is BACnet over IP over 10/100 Mbps.

2A-JACE: Programmable Tier 2A controller. No analog inputs or outputs. Primary networking is proprietary over IP over 10/100 Mbps Ethernet. For a small field control system, this might be the Tier 3 FPOC.

2C-FS: A Tier 2C gateway (application layer proxy). The Tier 2 network is Modbus over IP over 10/100 Mbps Ethernet. The Tier 1 network is proprietary over proprietary 2-wire media.

Figure 7 – Tier 2: IP portion of the Field Control System

1A-VAV: VAV box controller with multiple analog inputs and outputs. Also incorporates dedicated actuator and pressure sensor (normally Tier 0 devices). Network is LonTalk over TP/FT-10 media at 78 Kbps.



1A-LGR: Programmable controller with no analog inputs or outputs. Primary network is BACnet over Ethernet (not IP) media at 10/100 Mbps. Also supports BACnet over MS/TP media and proprietary protocol over RS-485 media. Can also be in Tier 2.

1N-Lswitch: LonTalk router between 2 TP/FT-10 (media) network segments. Also has RS-232 console port for configuration (generally not used).

Figure 8 – Tier 1: Non-IP portion of the Field Control System

0-Temperature: Thermistor temperature sensor (non-linear resistance change with temperature).

0-Actuator: Motor and valve assembly, with mechanical position indicator. 0 – 10 VDC or 4-20 mA analog input signal.

0-Actuator: Electric motor taking 4-20 mA or 0-10 VDC analog input signal and producing a 90 degree rotation.

Figure 9 – Tier 0: Sensors and Actuators

The ICS Architecture is described in five Tiers (and multiple sub-tiers), where each tier represents a collection of components that can be logically grouped together by function and IA approach. There are several critical considerations to the tiered architecture:

1) Not every implementation of an ICS will make use of every tier;
2) The same device may reside in different tiers, depending on its configuration. For example, some BACnet controllers may support different networks based on a dual in-line packet (DIP) switch, and thus the same device could reside in either Tier 1 or Tier 2.
3) In some cases, a single device may simultaneously fit into two principal tiers. For example, a device may act as both a Tier 2 controller and a Tier 3 Facility Point of Connection (FPOC).
4) In many cases, a device will fit multiple sub-tiers within the same principal tier, usually within Tier 2. For example, a Tier 2A BACnet controller will often act as a Tier 2C router to a Tier 1 network beneath it.
5) A single device may belong in different tiers, depending on the specific architecture. For example, the Tier 2A/2C controller in the example above may, in a small system, be the only IP device, in which case it is ***also*** the Tier 3 FPOC. In a larger system, there would be multiple IP devices and the upstream IP device (EUB switch or router) would be the Tier 3 FPOC.

Tier	Functional Description	Implemented Via	Installed By	Example Components	IA Considerations
5 **"External" Connection and Platform Information Technology (PIT) Management** **(“External Connection Between PIT and IP Network External to PIT)** **Platform IT System Management**	In many architectures, this tier provides the enclave boundary defense between the PIT (at Tiers 4 and below) and IP networks external to the PIT. (In other architectures, this boundary defense occurs in the external network). In many cases, there is a component within the PIT which would reside in Tier 5. This tier may be absent for a variety of reasons: there may not be an external connection, or the connection may be handled in the external network. Generally speaking from the perspective of ICSs functionality, this connection should be severely restricted, if not eliminated entirely. The ICSs can function in a completely isolated configuration. Additional functionality allowed through external connections includes: • Sending alarm notification using outbound access to a SMTP email server. • Upload of historical data and meter data to an enterprise server using outbound HTTP/HTTPS access for uploading. Often it is desirable to allow inbound HTTP from web clients (essentially Tier 4B clients, but on the external network) to the Tier 4A server, but this is not required. The Tier 5 PIT will likely be designated as an Installation Processing Node (IPN).	• Firewalls • DMZ/Perimeter Networking • Proxy Servers • Domain Controller, etc.	• IT and communications staff and contractors.	• Wide area networks (WANs) • Metropolitan area networks (MANs) • Local area networks (LANs) • Campus area networks (CANs) • Virtual private networks (VPNs) • Point of Presence • Demarcation Point or Main Point of Presence	This Tier should implement a "deny all / permit exception" policy to protect the PIT from the external network and the external network from the PIT.

4

UMCS Front End and IP Network

4N – UMCS IP Network – PIT Network

4A – M&C Server (Including Any Web Server, Data Historian, Etc.)

4B – OWS

(Tier 4A and 4B) The multi-facility operator interface for the system. This is typically a web-based client-server system with the clients at Tier 4B and the server(s) at Tier 4A. Some functions of the UMCS are:

- Providing graphical screens for monitoring and control of the system
- Allowing operators to schedule systems, set up historical trends, and respond to alarm conditions
- Provide for and support global control and optimization strategies that are impractical to implement within the control systems
- Provide connections to external systems such as maintenance scheduling programs and proactive diagnostics

The **Tier 4N** network is the network that connects multiple facility networks into a common base-wide network.

The Tier 4N network may either be a physically dedicated network or a dedicated virtual local area network (VLAN) utilizing the standard base-wide IP network as a transport layer.

- The network (Tier 4N) is typically government furnished.
- The computers, especially the clients in Tier 4B, are often government furnished.
- The software application is typically provided, installed and configured by the controls vendor.

Note that later connections between the UMCS and additional field control systems projects may be made by a variety of mechanisms.

- OT server racks
- GUI and HMI displays
- Fire alarm panels
- Radio base stations

The OT racks, hardware and software will likely be located in an Energy Operations Center, Campus Wide Operations Center, or Regional Operations Center and designated as a Special Purpose Processing Node (SSPN).

Tier 4 is where the ICSs most closely resembles a "standard" information system, and most IA controls can be applied at this tier. It's critical to remember that ICS is NOT a standard IS, however, and that controls must be applied in such a way as to not hamper the availability of the system. For example, some ICSs require software updates from the manufacturer prior to the implementation of a Java patch, and controls relating to the application of patches must not be implemented in a manner that requires automatic or immediate patching without ensuring that this won't cause the system to go offline.

	For each field control system, the FPOC is the specific single demarcation point in the OT system between that field control system and the front end system. It may be a gateway that translates data from one protocol to another. It generally has IA components in that it restricts access (by user, protocol, or specific commands) between tiers above and tiers below. From a control architecture perspective, it often looks and functions identically to a Tier 2C device. For a non-IP network (Tier 1), the FPOC is the device that connects the non-IP network to IP. For an IP network (Tier 2), the FPOC is the device located at the single connection point between the IP network in Tier 2 and the UMCS IP network; this is typically the upstream IP networking hardware (EUB switch or router).	Wide variety of devices depending on the specific architecture and protocols used: • Ethernet switch or IP router (any place there is a Tier 2 IP network) • Local operation network (Lon) (field control network) to Lon/IP router • Dedicated hardware gateway between proprietary field network and BACnet/IP • Application proxy providing enclave boundary defense between non-critical Lon/IP UMCS network and a critical Lon field control network • Tier 2D stand-alone front end for a local field control system	• Installation network staff • Controls contractor • System integrator when the field control system is connected to (integrated with) the front end system.	• Standard IT Ethernet switch • Echelon iLON 600 router • ALC LGR BACnet controller (IP to MS/TP router)	This device is critical from an IA perspective as it is where the dedicated local field control network connects to the base-wide network. Normally, securing this device protects the base-wide network from the local field systems (which often have a difficult time meeting IA controls). Occasionally, where there is a critical field control system, this device can protect the more critical field control system from the less-secure base-wide system (i.e., where there are 99 non-critical systems and 1 critical one, isolate the 1 from the 99 rather than try and secure the 99).
3 **Facility Points of Connection (FPOCs)**	In many cases, there is a ***single*** Tier 2A controller in the system (generally with a Tier 1 network beneath it). In these cases, we may consider the controller the FPOC, or we may consider the upstream IP networking hardware (EUB switch or router) to be the FPOC. Similarly, a device normally at Tier 2C could be the Tier 3 FPOC. Finally, we may have a Tier 2D computer which is the only IP device in the stand alone system; this may be considered the FPOC. *Note that a large base-wide system will have hundreds of these devices, one at each connection of a field control system to the base-wide system.*				This device should, in effect, have a "deny all / permit exception" policy applied. In many cases, this is inherent in the design of the network – a Tier 1 (non-IP) network inherently "denies" all protocols other than its specific control protocol. In other cases, this device may be a gateway ("application layer proxy") that does not permit any networking traffic through it, and only supports a very limited set of control functionality to pass. These devices tend to be very "dumb" devices and may not support many of the IA controls, but the critical "deny all / permit exception" approach should be designed into the device. Where this tier is an upstream IT device, it should be set up with the most restrictive set of access control list (ACL) possible.

2

IP Portion of the Field Control System

2N – IP Field Control Network (FCN)

2A – IP Based Networked Controllers

2B – Field Control Network Ethernet Hardware

2C – IP to Non-IP Control Protocol Routers or Control Protocol Gateways

2D – Field Control System Local Computers (Front-Ends, Engineering Tools)

(Tier 2A) This Tier (along with Tier 1) is where the control logic resides and where it gets converted to/and from electrical signals and can have the first IP connections. This is the portion of the OT system where:

- Analog electrical signals (from sensors) get converted to digital signals via A-D converters (although not all controllers will have hardware inputs).
- Digital information is converted to analog electrical signals (to actuators) via D-A converters (although not all controllers will have hardware outputs).
- Digital information is transmitted and received over a network.
- Digital information is processed according to a user-defined sequence to generate new digital information.
- These devices may incorporate integral Tier 0 sensors and actuators, for example, the Variable Air Volume (VAV) box controller shown incorporates an electric actuator.

Note that while there is exchange of data over the network, good design practice dictates (and DoD Guide Specifications require) that most of the data processing occurs using local sensor data and local actuator outputs; the system is designed to minimize dependence on networked data.

Tier 2C may also contain control protocol routers and/or control protocol gateways between tiers 1 and 2. These devices are generally physically part of a Tier 2A controller. In addition, from an IA perspective, they appear much the same as a Tier 2A controller.

(Tier 2D) In some cases, for either legacy or stand-alone systems (not necessarily isolated, but stand alone in that they do not rely on another system such as an UMCS), the front end operator interface may be physically local to that system. In this case, the operator interface is considered to be part of Tier 2 since it does not ride over the UMCS IP network.

(Tier 2A) Firmware-based dedicated digital processors, typically equipped with multiple analog inputs and outputs and corresponding A-D and D-A converters. These devices are driven by cost to have the minimal functionality for the application and are very constrained in RAM, processing power, and network I/O. In addition, these devices come in a vast variety of architectures, processors, vendors, and firmware. Aside from the fact that they use IP and are generally more powerful than Tier 1A devices, they are otherwise identical to Tier 1A devices. Many devices are available as either Tier 1A or 2A devices, where the hardware is identical except for the transceiver; some can even be field-configured for one or the other.

The Tier 2N network is generally Ethernet and the Tier 2B network hardware is standard IT network hardware, though generally with reduced functionality. For example, there may not be any requirement for remotely managed switches. Similarly, there is seldom a need for an IP router, since field control systems generally reside within a single (private) IP subnet.

The Tier 2 network (2N and 2B) uses IP, generally over Ethernet, such as BACnet/IP or Lon/IP.

While functionally, Tier 2D components act similarly to computers at Tier 4, the fact that they are local to (and dedicated to) a specific control systems means that from an IA perspective, they are better addressed as Tier 2 components. Tier 2D computers will often have another network logically beneath them, most often a non-IP network (and thus also function as Tier 2C devices).

- Controls contractor during installation or renovation of underlying mechanical or electrical system
- Generally during new building construction or major renovation

- **Tier 2A:**
  - Major air handling unit (AHU) controller,
  - Supervisory Controller
  - Electric meter (IP)
- **Tier 2B:**
  - "Dumb" Ethernet switch
- **Tier 2C:**
  - BACnet MS/TP to BACnet/IP router
  - Gateway between non-standard, non-IP protocol and a standard control protocol over IP
- **Tier 2D:**
  - Control system at a central plant where the nature and criticality of the system requires a local operator interface

Since it contains a variety of components from controllers (Tier 2A) to computers (Tier 2D), there is a variety of IA considerations for this tier. Many of the controllers will have the same limitations as the controllers in Tier 1, where most IA controls cannot/or will not apply to them. Some controllers will have significantly more capability, however, and additional controls will be applicable. In either case, the controllers should disable any network connections or services not required for operation of the OT system.

In some systems, particularly legacy systems, the computers at Tier 2D may be running an older operating systems and may not support some of the IA controls. In this case, the controls which can be applied without negatively affecting the availability of the system should be applied, and mitigating controls and measures should be taken when otherwise needed. Generally this will consist of further isolating the legacy systems.

1 **Non-IP Portion of the Field Control System** **1N – Network (Non-IP)** **1A – Networked Controllers** **(Non-IP)**	**(Tier 1A)** This is where the control logic resides and gets converted to/from analog electrical signals, as well as the portion of the OT system where: • Analog electrical signals (from sensors) get converted to digital signals via analog-to-digital (A-D) converters* • Digital information is converted to analog electrical signals (to actuators) via digital-to-analog (D-A) converters * • Digital information is transmitted and received over a network • Digital information is processed according to a user-defined sequence to generate new digital information • Devices may incorporate integral Tier 0 sensors and actuators, for example, a variable air volume (VAV) box controller incorporates an electric actuator **Note that not all controllers will have hardware inputs.* *Note that while there is exchange of data over the network, good design practice dictates (and DoD Guide Specifications require) that most of the data processing occurs using local sensor data and local actuator outputs; the system is designed to minimize dependence on networked data.* **(Tier 1N)** The Tier 1 network (media and hardware) does not use IP. It uses a variety of media at layers 1 and 2 (some standard, some not) and it uses layer 3 protocols other than IP. Some examples are: • BACnet over MS/TP, or BACnet over ARCnet • LonTalk over TP/FT-10 or LonTalk over TP/XF-1250 • Modbus over RS-485 For this reason, it is generally very specific to the control application and cannot be used for "standard" IT protocols and applications.	**(Tier 1A)** Firmware based dedicated digital processors, typically equipped with multiple analog inputs and outputs and corresponding A-D and D-A converters. These devices are driven by cost to have the minimal functionality for the application and are very constrained in random access memory (RAM), processing power, and network input/output (I/O). In addition, these devices come in a vast variety of architectures, processors, vendors, and firmware. **(Tier 1N)** The network media and hardware is similarly dedicated to that specific control protocol. There are layer 2 and layer 3 network devices made by a variety of vendors.	• Controls contractor during installation or renovation of underlying mechanical or electrical system • Generally during new building construction or major renovation	• VAV box controllers • Networked (non-IP) electric meter • Intelligent (networked) thermostat • LonWorks TP/XF-1250 (media) to TP/FT-10 (media) layer 3 router	Since devices (controllers) in this tier tend to be simpler devices, often few IA controls can be applied, particularly after the system has been designed and installed. Some basic controls/measures that can be applied at this tier include: • Disabling (or at a minimum prohibiting) secondary network connections (connections other than to the Tier 1 network) • The use of passwords on devices such as displays (to the capability supported by the device – many of which do not permit 14 character passwords, for example) • The application of physical security measures – which will be dictated and implemented by the underlying equipment

0 **Sensors and Actuators** **"Dumb" Non-Networked Sensors and Actuators**	The interface between the OT system and the underlying controlled process / equipment where electrical signals in the control system get converted to/from physical values and actions in the underlying controlled system.	Devices which: • Convert physical properties (e.g., temperature, pressure, etc.) to an analog electrical signal* • Take an analog electrical signal* and produce a physical action (e.g., open / close a valve or damper, etc.) ** Note that these electrical signals are purely analog – there are no digital signals at this tier and hence no networking. Also note that there are "smart" sensors, which include a sensor (or actuator) with a controller. These devices are considered to be Tier 1A or Tier 2A devices.*	• Controls contractor during installation or renovation of underlying mechanical or electrical system • Generally during new building construction or major renovation	• Temperature sensor (thermistor, RTD) • Mechanical actuator (for damper or valve) • Thermostat • Pressure sensor • Pulse-output meter	In general IA controls do not apply to this tier, since there is no network communication and no "intelligence" in the components at this tier. While physical security is a consideration, these devices are attached to the mechanical/electrical system and physical security is dictated and implemented based on the underlying equipment.

Mission Criticality

The objective of this overlay is to develop the baseline of Low, Moderate, and High Impact ICSs, and define the accreditation boundary and types of devices typically found on an ICS. A Low Impact ICSs addresses the "80%" non-critical systems (i.e., typical office, administrative, housing, warehouse, et al. buildings control systems). Many of the Moderate and High Impact systems are listed as Task Critical Assets in the Defense Critical Infrastructure Protection (DCIP) program, and are classified at the Secret level or higher. Figure 10 illustrates the conceptual types of ICSs and criticality. There are approximately 400 plus major military installations and operating sites. For this Overlay, the ICS systems PIT boundary is defined as the Enclave and Installation Processing Node. Currently, there are 611 controls in the CNSSI 1253, of which 197 have been determined to apply for ICSs.

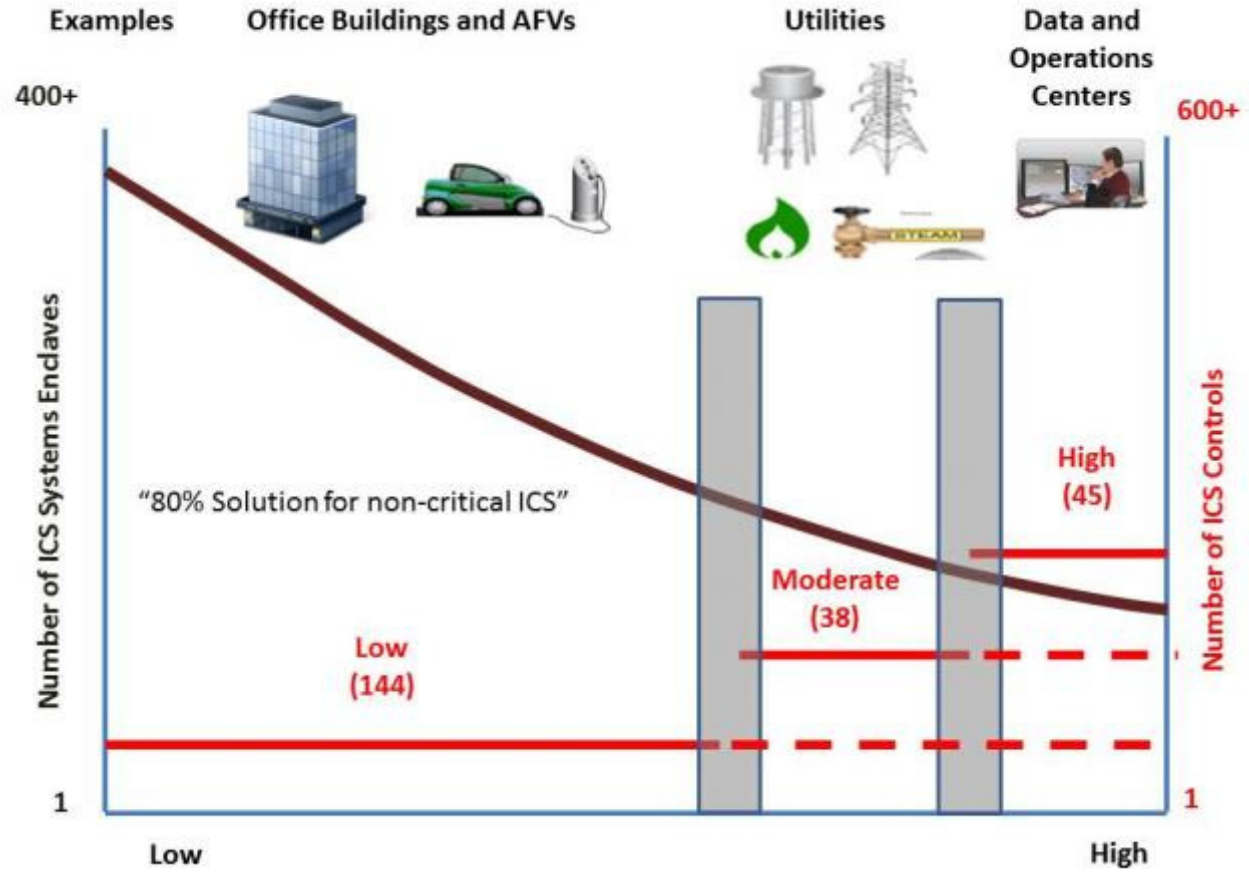


Figure 10 – ICSs Criticality

For ICSs systems, it is extremely important to recognize that *availability* is often of much more significance than *confidentiality* or *integrity*. Additionally, ICS systems do not have a distinct

cutoff for criticality, but rather span a range. For example, an electric utility SCADA system may be a Mission Dependent primary system that supports a Mission Critical Data Center system with secondary generator back up, but if primary power is lost, the system will have degraded capability, and restoration of the primary electric is essential for long-term mission completion.

2. Applicability

The following questions are used to determine whether or not this overlay applies to a Low Impact ICS system:

1. Does the ICS have a CNSSI 1253 C-I-A rating of Low-Low-Low or less, where "loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals"?
2. Is the ICS part of a real property asset listed in the DoD Federal Real Property Profile (FRPP) and listed as "Not Mission Dependent – **mission unaffected**"?
3. Is the ICS designated a prior DoD Information Assurance Certification and Accreditation Process (DIACAP) "Mission Assurance Category 3 – These systems handle information that is necessary for the conduct of day-to-day business, but **does not materially affect** support to deployed or contingency forces in the short-term"?

- **If the answer is yes to any of the questions, STOP here and use the Low Impact overlay.**

The following questions are used to determine whether or not this overlay applies to a Moderate ICS system:

1. Does the ICS have a CNSSI 1253 C-I-A rating of Moderate-Moderate-Moderate or less, where "loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals"?
2. Is the ICS part of a real property asset listed in the DoD FRPP and listed as "Mission Dependent, Not Critical – **does not fit into Mission Critical or Not Mission Dependent** categories"?
3. Is the ICS designated a prior DIACAP "Mission Assurance Category 2 – Systems handling information that is important to the support of deployed and contingency forces. **Loss of availability is difficult to with and can only be tolerated for a short time**"?
4. Has the installation commander designated the ICS as producing critical information?

- **If the answer is yes to any of the questions, STOP here and use the Moderate Impact overlay.**

The following questions are used to determine whether or not this overlay applies to a High ICS system:

1. Does the ICS have a CNSSI 1253 C-I-A rating of High-High-High or less, where "loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals"?
2. Is the ICS part of a real property asset listed in the DoD FRPP and listed as "Mission Critical – without constructed asset or parcel of land, mission is compromised"?
3. Is the ICS designated a prior DIACAP "Mission Assurance Category 1 – Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss or availability are unacceptable and could include the immediate and sustained loss of mission effectiveness"?
4. Is the ICS a DCIP Tier 1 Task Critical Asset listed as "an asset, the loss, incapacitation, or disruption of which could result in mission (or function) failure at the DoD, Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure level"?
5. Is the ICS a DCIP Tier 2 Task Critical Asset listed as "an asset, the loss, incapacitation, or disruption of which could result in severe mission (or function) degradation at the DoD, Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure level"?
6. Is the ICS a DCIP Tier 3 Task Critical Asset listed as "an asset, the loss, incapacitation, or disruption of which could result in mission (or function) failure below the DoD, Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure level"?
7. Has the installation commander designated the ICS as producing critical information?

- **If the answer is yes to any of the questions, the High Impact overlay applies. In some of the highest criticality installations the addition of controls during tailoring (above and beyond the overlay) will be required.**

If you did not answer yes to any of these questions, go back and re-evaluate your answers to the questions related to Low and Moderate systems.

3. Implementation

The ICS-PIT Overlay is based on:

- ANSI/ISA 99.00.01 2007 *Security for Industrial Automation and Control Systems*
- CNSSI No. 1253, Revision 1.1, *Security Controls and Control Selections for National Security Systems*, March 2012

- Council on Environmental Quality (CEQ), Adjunct to Executive Order 13514, *Implementing Instructions – Sustainable Locations for Federal Facilities*, September 15, 2011
- DoD Unified Facility Criteria 3-470-01, *LonWorks Utility Monitoring and Control System (UMCS)*, May 2012
- DoD Unified Facility Criteria 4-010-01, *Minimum Antiterrorism Standards for Buildings,* February 2012
- DoD Unified Facility Criteria 4-022-01, *Security Engineering Manual*, March 2005
- DoD *Unified Facility Guide Specification 25-10-10, Utility* Monitoring and Control System, October 2012
- Energy Sector Control Systems Working Group, *Roadmap to Secure Energy Delivery Systems*, January 2011
- Executive Order 13514, *Federal Leadership in Environmental, Energy and Economic Performance*, October 2009
- Executive Office of the President of the United States, *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*, June 2011
- FEMA 426, *Reference Manual to Mitigate Buildings Against Terrorist Attack*, December 2003
- International Building Code
- National Defense Authorization Act, 2010
- National Fire Protection Association (NFPA) 70, *National Electric Code*, Current Edition (2011)
- NFPA 1, *National Fire Code,* Current Edition (2012)
- National Science and Technology Council Committee on Technology, *Submetering of Building Energy and Water Usage*, October 201*1*
- National Institute of Standards and Technology (NIST) SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
- NIST SP 800-53, Revision 4 Draft, *Recommended Security Controls for Federal Information Systems and Organizations*, February 2012
- NIST SP 800-82, *Guide to Industrial Control Systems (ICSs) Security*, June 2011
- NIST 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011
- NISTR 7628, *Guidelines for Smart Grid Cyber Security*, September 2010
- NISTR Draft 7823 *Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework*, July 2012
- NIST SP 1108R2, *Framework and Roadmap for Smart Grid Interoperability Standards*, Release 2.0, February 2012

The ICS Overlay can apply to all the baselines defined in CNSSI No. 1253. The overlay does not require any other overlays to provide the needed protection for systems within ICS environments. Care should be taken when tailoring information systems that contain ICS information, since numerous security controls are required by legislation, building code, and transportation code. See Section 7 for the list of security controls required to meet regulatory/statutory requirements.

4. Table of Overlay Controls

The tables below contain the security controls to be tailored from a CNSSI baseline for Low, Moderate, and High Impact ICS systems:

1. For Low Impact systems, start with a CNSSI L-L-L baseline and use the "Low Overlay" column. Note that the Low Overlay only removes controls (--); there are no additions.
2. For Moderate Impact systems, start with a CNSSI M-M-M system and use the “Moderate Overlay" column. Note that the Moderate Overlay only removes controls (--); there are no additions.
3. For High Impact systems, start with a CNSSI H-H-H system and the "High Overlay" column. Note that the High Overlay only removes controls (--); there are no additions.

Table 2: ICS Systems Overlay Security Controls

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
AC-2(1)	--	NA	NA
AC-2(2)	--	NA	NA
AC-2(3)	--	NA	NA
AC-2(4)	--	NA	NA
AC-2(7)	--	NA	NA
AC-3(4)	--	NA	NA
AC-3(6)	NA	NA	--
AC-4	--	NA	NA
AC-5	--	NA	NA
AC-6(1)	--	NA	NA
AC-6(2)	--	NA	NA
AC-6(5)	--	NA	NA
AC-6(6)	NA	NA	--
AC-9	NA	--	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
AC-17(1)	--	NA	NA
AC-17(4)	--	NA	NA
AC-17(5)	--	NA	NA
AC-17(6)	--	NA	NA
AC-17(7)	--	NA	NA
AC-18(2)	--	NA	NA
AC-18(4)	--	NA	NA
AC-18(5)	--	NA	NA
AC-19(1)	--	NA	NA
AC-19(2)	--	NA	NA
AC-19(4)	--	NA	NA
AC-20(2)	--	NA	NA
AT-3(2)	--	NA	NA
AT-5	--	NA	NA
AU-2(3)	--	NA	NA
AU-2(4)	--	NA	NA
AU-3(1)	--	NA	NA
AU-3(2)	--	NA	NA
AU-5(1)	--	NA	NA
AU-5(2)	NA	--	NA
AU-6(3)	--	NA	NA
AU-7(1)	NA	--	NA
AU-8(1)	--	NA	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
AU-9(4)	--	NA	NA
AU-10	NA	--	NA
AU-10(5)	NA	--	NA
CA-2(1)	--	NA	NA
CA-3(1)	--	NA	NA
CA-3(2)	NA	--	NA
CA-7(1)	--	NA	NA
CA-7(2)	--	NA	NA
CM-2(5)	--	NA	NA
CM-3(4)	--	NA	NA
CM-4(2)	--	NA	NA
CM-5(1)	--	NA	NA
CM-5(2)	--	NA	NA
CM-5(5)	--	NA	NA
CM-5(6)	--	NA	NA
CM-6(3)	--	NA	NA
CM-7(1)	--	NA	NA
CM-7(3)	--	NA	NA
CM-8(4)	--	NA	NA
CM-8(5)	--	NA	NA
CM-9	--	NA	NA
CP-6	NA	--	NA
CP-6(1)	NA	--	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
CP-6(2)	NA	NA	--
CP-6(3)	NA	--	NA
CP-7	NA	--	NA
CP-7(1)	NA	--	NA
CP-7(2)	NA	--	NA
CP-7(3)	NA	--	NA
CP-7(4)	NA	--	NA
CP-7(5)	NA	--	NA
CP-8(1)	NA	--	NA
CP-8(2)	NA	--	NA
CP-9(1)	--	NA	NA
CP-10(2)	--	NA	NA
IA-2(5)	--	NA	NA
IA-2(8)	--	NA	NA
IA-3	--	NA	NA
IA-3(1)	--	NA	NA
IA-3(2)	--	NA	NA
IA-3(3)	--	NA	NA
IA-4(4)	--	NA	NA
IA-5(2)	--	NA	NA
IA-5(3)	--	NA	NA
IA-5(4)	--	NA	NA
IA-5(6)	--	NA	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
IA-5(7)	--	NA	NA
IA-5(8)	--	NA	NA
IR-3	--	NA	NA
IR-4(1)	--	NA	NA
IR-4(3)	--	NA	NA
IR-4(4)	--	NA	NA
MA-2(1)	--	NA	NA
MA-2(2)	NA	NA	--
MA-3	--	NA	NA
MA-3(1)	NA	--	NA
MA-3(2)	--	NA	NA
MA-3(3)	--	NA	NA
MA-4(2)	--	NA	NA
MA-4(3)	--	NA	NA
MA-4(5)	--	NA	NA
MA-4(6)	--	NA	NA
MA-4(7)	--	NA	NA
MA-5(1)	--	NA	NA
MP-3	--	NA	NA
MP-4	--	NA	NA
MP-4(1)	NA	NA	--
MP-5	--	NA	NA
MP-5(2)	--	NA	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
MP-6(2)	--	NA	NA
MP-6(3)	--	NA	NA
MP-6(4)	--	NA	NA
MP-6(5)	--	NA	NA
MP-6(6)	--	NA	NA
PE-2(3)	--	NA	NA
PE-3(2)	--	NA	NA
PE-3(3)	--	NA	NA
PE-5	--	NA	NA
PE-9	--	NA	NA
PE-9(2)	NA	--	NA
PE-10	--	NA	NA
PE-19	NA	--	NA
PE-19(1)	NA	--	NA
PL-2(1)	--	NA	NA
PL-2(2)	--	NA	NA
PL-6	--	NA	NA
PS-3(1)	--	NA	NA
PS-3(2)	--	NA	NA
PS-6(1)	--	NA	NA
PS-6(2)	--	NA	NA
RA-5(1)	--	NA	NA
RA-5(2)	--	NA	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
RA-5(4)	--	NA	NA
RA-5(5)	--	NA	NA
RA-5(7)	--	NA	NA
SA-4(6)	--	NA	NA
SA-5(1)	--	NA	NA
SA-5(2)	--	NA	NA
SA-9(1)	--	NA	NA
SA-10	--	NA	NA
SA-10(1)	--	NA	NA
SA-11	--	NA	NA
SA-12	--	NA	NA
SA-12(2)	--	NA	NA
SC-2	--	NA	NA
SC-2(1)	--	NA	NA
SC-4	--	NA	NA
SC-5(1)	--	NA	NA
SC-7(1)	--	NA	NA
SC-7(2)	--	NA	NA
SC-7(4)	--	NA	NA
SC-7(5)	--	NA	NA
SC-7(7)	--	NA	NA
SC-7(8)	--	NA	NA
SC-7(12)	--	NA	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
SC-7(11)	--	NA	NA
SC-7(13)	--	NA	NA
SC-7(14)	--	NA	NA
SC-8	--	NA	NA
SC-8(2)	NA	NA	--
SC-9	--	NA	NA
SC-9(1)	--	NA	NA
SC-9(2)	NA	--	NA
SC-10	--	NA	NA
SC-11	--	NA	NA
SC-12(1)	--	NA	NA
SC-15	--	NA	NA
SC-15(1)	--	NA	NA
SC-15(2)	--	NA	NA
SC-15(3)	--	NA	NA
SC-17	--	NA	NA
SC-18(1)	--	NA	NA
SC-18(2)	--	NA	NA
SC-18(3)	--	NA	NA
SC-18(4)	--	NA	NA
SC-19	--	NA	NA
SC-21	--	NA	NA
SC-21(1)	--	NA	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
SC-22	--	NA	NA
SC-23	--	NA	NA
SC-23(1)	--	NA	NA
SC-23(2)	--	NA	NA
SC-23(3)	--	NA	NA
SC-23(4)	--	NA	NA
SC-24	--	NA	NA
SC-28	--	NA	NA
SC-32	NA	--	NA
SI-2(3)	--	NA	NA
SI-2(4)	--	NA	NA
SI-3(1)	--	NA	NA
SI-3(2)	--	NA	NA
SI-3(3)	--	NA	NA
SI-4(1)	--	NA	NA
SI-4(2)	--	NA	NA
SI-4(4)	--	NA	NA
SI-4(5)	--	NA	NA
SI-4(7)	--	NA	NA
SI-4(8)	--	NA	NA
SI-4(9)	--	NA	NA
SI-4(11)	--	NA	NA
SI-4(12)	--	NA	NA

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
SI-4(14)	--	NA	NA
SI-4(15)	--	NA	NA
SI-4(16)	--	NA	NA
SI-4(17)	--	NA	NA
SI-5(1)	--	NA	NA
SI-6	--	NA	NA
SI-6(1)	--	NA	NA
SI-6(3)	--	NA	NA
SI-8	--	NA	NA
SI-8(1)	--	NA	NA
SI-8(2)	--	NA	NA
SI-10	NA	--	NA
SI-11	--	NA	NA
PM-8	--	NA	NA

5. Supplemental Guidance

The security controls and control enhancements are likely candidates for tailoring, with the applicability of scoping guidance indicated for each control/enhancement. The citation of a control without enhancements (e.g., AC-17) refers only to the base control without any enhancements, while reference to an enhancement by a parenthetical number following the control identification (e.g., AC-17(1)) refers only to the specific control enhancement.

Organizations are required to conduct a risk assessment, taking into account the tailoring and supplementation performed in arriving at the agreed-upon set of security controls for the ICS, as well as the risk to the organization's operations and assets, individuals, other organizations, and the Nation being incurred by operation of the ICS with the intended controls. Based on an evaluation of the risk, the organization will further tailor the control set obtained using this overlay by adding or removing controls in accordance with the CNSSI 1253 process. The addition or removal of controls during tailoring requires justification.

ICS supplemental guidance provides organizations with additional information on the application of the security controls and control enhancements to ICSs and the environments in which these specialized systems operate. The supplemental guidance also provides information as to why a particular security control or control enhancement may not be applicable in some ICSs environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls).

The systems controls supplemental guidance provided below is a combination of NIST 800-53 Rev 3 Appendix I, and the DoD ICSs-PIT Technical Working Group decision to include definitive text for each control as well as guidance on how to apply a control for OT and the unique DoD environment. Refer to Figure 3 – ICS Tiers diagram and Table 3 for the Tier definitions.

Table 3: ICSs Tiers Definitions

Tier	Description
	IP Network External to PIT
5	**"External" Connection and PIT Management**
	"External" Connection (between PIT and IP Network External to PIT)
	Platform IT System Management
4	**UMCS Front End and IP Network**
4N	UMCS IP network -- PIT Network
4A	M&C Server (including any web server, data historian, etc.)
4B	OWS
3	**Facility Points Of Connection (FPOCs)**
2	**IP Portion of the Field Control System**
2N	IP Field Control Network (FCN)
2A	IP based networked controllers
2B	Field control network Ethernet hardware
2C	IP to non-IP control protocol routers or control protocol gateways
2D	Field control system local computers (front-ends, engineering tools)
1	**Non-IP portion of the Field Control System**
1N	Network (non-IP)
1A	Networked controllers (non-IP)
0	**"DUMB" non-networked sensors and actuators**

LOW IMPACT SYSTEMS

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization has policies and procedures in place to restrict physical access to the ICS (e.g., workstations, hardware components, field devices) and predefine account privileges. Where the ICS (e.g., certain remote terminal units, meters, relays) cannot support account management, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, intrusion detection, auditing measures) in accordance with the general tailoring guidance.

Applies to Tiers 2a, 2d, 3, 4a, and 4b

AC-2 ACCOUNT MANAGEMENT

ICS Supplemental Guidance: In situations where physical access to the ICS (e.g., workstations, hardware components, field devices) predefines account privileges or where the ICS (e.g., certain remote terminal units, meters, relays) cannot support account management, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, intrusion detection, auditing measures) in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a, and 4b

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support the use of automated mechanisms for the management of ICS accounts, the organization employs non-automated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-3 ACCESS ENFORCEMENT

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS.

Applies to Tiers 2a, 2d, 3, 4a, and 4b

References: NIST Special Publication 800-82

AC-6 LEAST PRIVILEGE

ICS Supplemental Guidance: In situations where the ICS cannot support differentiation of privileges, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing) in accordance with the general

tailoring guidance. The organization carefully considers the appropriateness of a single individual having multiple critical privileges.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

ICS Supplemental Guidance: In situations where the ICS cannot support account/node locking or delayed login attempts, or the ICS cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., logging or recording all unsuccessful login attempts and alerting ICS security personnel though alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded) in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a and 4b

AC-8 SYSTEM USE NOTIFICATION

ICS Supplemental Guidance: In situations where the ICS cannot support system use notification, the organization employs appropriate compensating controls (e.g., posting physical notices in ICS facilities) in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a and 4b

AC-11 SESSION LOCK

ICS Supplemental Guidance: The ICS employs session lock to prevent access to specified workstations/nodes. The ICS activates session lock mechanisms automatically after an organizationally defined time period for designated workstations/nodes on the ICS. In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Session lock is not a substitute for logging out of the ICS. In situations where the ICS cannot support session lock, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance.

Applies to all Tiers

References: NIST Special Publication 800-82

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR UTHENTICATION

ICS Supplemental Guidance: The organization only allows specific user actions that can be performed on the ICS system without identification or authentication to be performed on non-IP sensor and actuator devices.

Applies to Tiers 4a and 4b

AC-17 REMOTE ACCESS

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Applies to Tier 4a

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization then explores all possible cryptographic mechanisms (e.g., encryption, digital signature, hash function), as each mechanism has a different delay impact. In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on safety, performance, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing for remote sessions or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: The organization restricts remote access to one approved method, with no backdoors or modems.

Control Enhancement: (8)

ICS Enhancement Supplemental Guidance: The organization disables networking protocols in accordance with DoDI 8551.1, except for explicitly identified components in support of specific operational requirements.

AC-18 WIRELESS ACCESS

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Applies to Tier 2 and 4

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity, and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization explores all possible cryptographic mechanisms (e.g., encryption, digital signature, hash function), as each mechanism has a different delay impact. In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of wireless access, or the components cannot use cryptographic mechanisms due to significant adverse impact on safety, performance, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing for wireless access or limiting wireless access privileges to key personnel) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: The organization disables wireless networking capabilities internally embedded within ICS components across all Tier levels, prior to issuance and deployment.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a, and 4b

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: Per DoD guidance, no USB thumb drives are authorized for use. Other authorized removable media must be identified with username and contact information.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

ICS Supplemental Guidance: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external ICS and must have a Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) and Service Level Agreement (SLA) between the ICS and Service Provider.

Applies to Tiers 4a and 5

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: The organization permits authorized individuals to use an external ICS to access the ICS or to process, store, or transmit organizationally controlled information only when the organization has an approved ICS connection or processing agreements with the organizational entity hosting the external ICS.

AC-22 PUBLICLY ACCESSIBLE CONTENT

ICS Supplemental Guidance: Generally, public access to ICS information is not permitted.

Applies to all Tiers

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. Supplemental IA training may be required specific to the systems accessed.

Applies to all Tiers

AT-2 SECURITY AWARENESS

ICS Supplemental Guidance: Security awareness training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

Applies to all Tiers

AT-3 SECURITY TRAINING

ICS Supplemental Guidance: Security training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security training program is consistent with the requirements of the security awareness and training policy established by the organization.

Applies to all Tiers

AT-4 SECURITY TRAINING RECORDS

ICS Supplemental Guidance: The organization, in conjunction with the Information Assurance Managers (IAMS), documents and monitors individual ICS security training activities, including basic security awareness training and specific ICS security training, and retains individual training records for at least 5 years. Federal employees and contractors that work on High Performance Green Buildings subject to the Federal Buildings Personnel Training Act will maintain their core competencies in www.fmi.gov.

Applies to all Tiers

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization, in conjunction with the IAMS, develops, disseminates, and annually reviews/updates a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also follows formal documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Applies to all Tiers

AU-2 AUDITABLE EVENTS

ICS Supplemental Guidance: Most ICS auditing occurs at the application level.

Applies to Tiers 2d, 4a, and 4b

AU-3 CONTENT OF AUDIT RECORDS

ICS Supplemental Guidance: The ICS produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. An ICS system usually has a front-end server(s), workstation(s) and possibly laptops that produce audit logs in great detail. Other ICS components are limited in what events can be audited; enabling auditing on controllers/PLCs can create a self-denial of service because the CPU and memory are limited.

Applies to Tiers 2d, 4a, and 4b

AU-4 AUDIT STORAGE CAPACITY

ICS Supplemental Guidance: The organization allocates audit record storage capacity, and in accordance with individual device design, configures auditing to reduce the likelihood of such capacity being exceeded.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

ICS Supplemental Guidance: In general, audit record processing is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing, including response to audit failures, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

Applies to all Tiers

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

ICS Supplemental Guidance: The organization reviews and analyzes ICS audit records every seven days for indications of inappropriate or unusual activity, and reports findings to designated organizational officials. The organization adjusts the level of audit review, analysis, and reporting within the ICS when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation, based on law enforcement information, intelligence information, or other credible sources of information.

Applies to Tiers 2d, 4a, and 4b

AU-8 TIME STAMPS

ICS Supplemental Guidance: The ICS uses internal system clocks to generate time stamps for audit records. The preferred method uses Network Timing Protocol (NTP) to synchronize servers and workstations. The ICS should have all of the internal clocks standardized to a specific time zone (GMT, ZULU, UTC, etc.) and all clocks must agree with each other, though they may not necessarily have the exact time.

Applies to Tiers 2d, 4a, and 4b

AU-9 PROTECTION OF AUDIT INFORMATION

ICS Supplemental Guidance: The ICS protects audit information and audit tools from unauthorized access, modification, and deletion. Auditing roles will be established on all devices that can be audited.

Applies to Tiers 2d, 4a, and 4b

AU-11 AUDIT RECORD RETENTION

ICS Supplemental Guidance: The organization retains audit records for one year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Applies to all Tiers

AU-12 AUDIT GENERATION

ICS Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs non-automated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a, and 4b(0)

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

Applies to all Tiers

CA-2 SECURITY ASSESSMENTS

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organization's information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken offline, or replicated to the extent feasible, before an assessment can be conducted. If an ICS must be taken offline to conduct an assessment, the assessment is scheduled to occur during planned ICS outages whenever possible. In situations where the organization cannot, for operational reasons, conduct a live assessment of a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct the assessment) in accordance with the general tailoring guidance.

Applies to all Tiers

CA-3 INFORMATION SYSTEM CONNECTIONS

ICS Supplemental Guidance: The organization authorizes connections from the ICS to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements such as an MOA/MOU and/or an SLA; documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and monitors the information system connections on an ongoing basis, verifying enforcement of security requirements.

Applies to Tiers 4a and 5

CA-5 PLAN OF ACTION AND MILESTONES

ICS Supplemental Guidance: The organization develops a plan of action and milestones for the ICS to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls, and to reduce or eliminate known vulnerabilities in the system. The organization updates existing plans of action and milestones (POA&M) at least every 90 days based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. The POA&M from the initial Risk Assessment (RA) will be used as the systems security lifecycle vulnerability and mitigation remediation tool. As ICS and IT technology changes regularly, the initial RA will be reviewed in order to determine how the POA&M should be revised to account for improvements or upgrades to legacy systems that might allow more stringent controls to be put into place without adversely affecting operations.

Applies to all Tiers

CA-6 SECURITY AUTHORIZATION

ICS Supplemental Guidance: The organization assigns a senior-level executive or manager to the role of authorizing official for the ICS; ensures that the authorizing official authorizes the ICS for processing before commencing operations; and updates the security authorization at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates. Federal employees (to include the AO and IA functions) and contractors that work on High Performance Green Buildings subject to the Federal Buildings Personnel Training Act will maintain their core competencies in www.fmi.gov.

Applies to all Tiers

CA-7 CONTINUOUS MONITORING

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organization's information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. Ongoing assessments of ICS may not be feasible. (See CA-2 ICS Supplemental Guidance in this Appendix.)

Applies to all Tiers

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented configuration management policy that addresses

purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. Configuration management of the field controllers must be carefully considered as they can have operations and maintenance ramifications; the ICS components must be quickly replaced or repaired to ensure the mission support is not affected or is the disruption is minimal.

Applies to all Tiers

CM-2 BASELINE CONFIGURATION

ICS Supplemental Guidance: The organization develops, documents, and maintains a current baseline configuration of the ICS under configuration control.

Applies to Tiers 2 and above

CM-3 CONFIGURATION CHANGE CONTROL

ICS Supplemental Guidance: The organization determines the types of changes to the ICS that are configuration controlled; approves configuration-controlled changes to the system with explicit consideration for security impact analyses; documents approved configuration-controlled changes to the system; retains and reviews records of configuration-controlled changes to the system; audits activities associated with configuration-controlled changes to the system; and coordinates and provides oversight for configuration change control activities through a configuration control board (CCB) that convenes at a frequency determined by the CCB.

Applies to Tiers 2d, 3, 4, and 5

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to implement configuration change control, the organization employs non-automated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-4 SECURITY IMPACT ANALYSIS

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies.

Applies to\Tiers 4a and 5

CM-5 ACCESS RESTRICTIONS FOR CHANGE

ICS Supplemental Guidance: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the ICS. Changes to an ICS should be documented on As-Built drawings and/or in Building Information Models.

Applies to Tiers 2d, 3, 4a, 4b, and 5

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to enforce access restrictions and support auditing of enforcement actions, the organization employs non-automated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-6 CONFIGURATION SETTINGS

ICS Supplemental Guidance: The organization establishes and documents mandatory configuration settings for ICS products employed within the ICS using DoD or DHS security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs, ICS-CERT, etc.) that reflect the most restrictive mode consistent with operational requirements; the organization implements the configuration settings; identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Applies to Tiers 2d, 3, 4a, 4b, and 5

CM-7 LEAST FUNCTIONALITY

ICS Supplemental Guidance: The organization configures the ICS to provide only essential capabilities and specifically prohibits or restricts the use of functions, ports, protocols, and/or services in accordance with DoDI 8551.01.

Applies to all Tiers

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

ICS Supplemental Guidance: The organization develops, documents, and maintains an inventory of ICS components that accurately reflects the current ICS that is IP-addressable; is consistent with the authorization boundary of the ICS; is at the level of granularity deemed necessary for tracking and reporting; includes hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, ICS/component owner, the machine name for a networked component/device, and is available for review and audit by designated organizational officials. A complete inventory of all field level devices, sensors and actuators should be in a Computerized Maintenance Management system, As-Built drawings, in a Building

Information Model, Builder, or in the Construction-Operations Building information exchange data (if used).

Applies to Tiers 2d, 3, and 4

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: The organization updates the inventory of ICS components as an integral part of component installations, removals, and ICS updates.

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. Because ICS are the foundational elements (power, water, HVAC, lighting, etc.) for all missions, the Continuity of Operations Plan (COOP) must be closely coordinated with the Defense Critical Infrastructure Protection Plan and critical ICS systems identified and prioritized for restoration of services.

Applies to all Tiers

CP-2 CONTINGENCY PLAN

ICS Supplemental Guidance: The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the ICS executes predetermined procedures (e.g., alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, alert the operator and then maintain the last operational setting prior to failure). Consideration is given to restoring system state variables as part of restoration (e.g., valves are restored to their original settings prior to the disruption).

Applies to all Tiers

References: NIST Special Publication 800-82

CP-3 CONTINGENCY TRAINING

ICS Supplemental Guidance: The organization trains personnel in their contingency roles and responsibilities with respect to the ICS and provides refresher training at least annually as defined in the contingency plan.

Applies to all Tiers

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

ICS Supplemental Guidance: In situations where the organization cannot test or exercise the contingency plan on production ICSs due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., using scheduled and unscheduled system maintenance activities including responding to ICS component and system failures, as an opportunity to test or exercise the contingency plan) in accordance with the general tailoring guidance.

Applies to all Tiers

CP-9 INFORMATION SYSTEM BACKUP

ICS Supplemental Guidance: The organization conducts backups of user-level information contained in the ICS at least weekly as defined in the contingency plan; conducts backups of system-level information contained in the ICS at least weekly and as required by system baseline configuration changes in accordance with the contingency plan; conducts backups of ICS documentation including security-related documentation when created or received, when updated, and as required by system baseline configuration changes in accordance with the contingency plan; and protects the confidentiality and integrity of backup information at the storage location.

Applies to Tiers 2d and 4a

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

ICS Supplemental Guidance: Reconstitution of the ICS includes restoration of system state variables (e.g., valves are restored to their appropriate settings as part of the reconstitution).

Applies to all Tiers

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Applies to all Tiers

IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. In situations where the ICS cannot support user identification and authentication, or the organization determines it is not advisable to perform user identification and authentication due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance. For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access. (See AC-17 ICS Supplemental Guidance in this Appendix.) Local user access to ICS components is enabled only when necessary, approved, and authenticated.

Applies to Tiers 2d, 4a, and 4b

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support multifactor authentication, the organization employs compensating controls in accordance with the general tailoring guidance (e.g., implementing physical security measures).

IA-4 IDENTIFIER MANAGEMENT

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based.

Applies to users connecting at Tiers 2d, 4a, and 4b

References: NIST Special Publication 800-82

IA-5 AUTHENTICATOR MANAGEMENT

ICS Supplemental Guidance: The organization manages ICS authenticators for users and devices by verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; establishing initial authenticator content for authenticators defined by the organization; ensuring that authenticators have sufficient strength of mechanism for their intended use; establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; changing default content of authenticators upon ICS installation; establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); changing/refreshing authenticators' Common Access Cards (CACs) every 3 years, or 1 year from term of contract, Password every 60 days, Biometrics every 3 years; protecting authenticator content from unauthorized disclosure and modification; and requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Applies to users connecting at Tiers 2d, 4a, and 4b

References: NIST Special Publication 800-82

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: The ICS, for password-based authentication: enforces minimum password complexity of as supported by the device a minimum of 15 Characters, 1 of each of the following character sets: Upper-case, Lower-case, Numerics, Special characters (e.g. ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [ ] / ? > <); enforces at least 50 % the number of changed characters when new passwords are created; encrypts passwords in storage and in transmission; enforces password minimum and maximum lifetime restrictions of minimum 24 hours, maximum 60 days; and prohibits password reuse for minimum of 5 generations.

IA-6 AUTHENTICATOR FEEDBACK

ICS Supplemental Guidance: The ICS obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. Field control system components (such as simple display panels) may not have this capability; users should shield the screen as passwords are entered.

Applies to all Tiers

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

ICS Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

Applies to Tiers 2d, 4a, and 4b

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

ICS Supplemental Guidance: The ICS uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Applies to Tiers 2d, 4a, and 4b

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among

organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Applies to Tiers 4a and 5

IR-2 INCIDENT RESPONSE TRAINING

ICS Supplemental Guidance: The organization trains personnel in their incident response roles and responsibilities with respect to the ICS; and provides refresher training annually.

Applies to Tiers 4a and 5

IR-4 INCIDENT HANDLING

ICS Supplemental Guidance: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; coordinates incident handling activities with contingency planning activities; and incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Applies to Tiers 2d, 4a, 4b and 5

IR-5 INCIDENT MONITORING

ICS Supplemental Guidance: The organization tracks and documents ICS security incidents. Security incidents and monitoring should be coordinated with the DHS ICS-CERT and USCYBERCOM ICS functional leads.

Applies to Tiers 2d, 4a, and 4b

IR-6 INCIDENT REPORTING

ICS Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) maintains the ICS Security Center at http://www.uscert.gov/control_systems.

Applies to all Tiers

References: NIST Special Publication 800-82

IR-7 INCIDENT RESPONSE ASSISTANCE

ICS Supplemental Guidance: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the ICS for the handling and reporting of security incidents.

Applies to all Tiers

IR-8 INCIDENT RESPONSE PLAN

ICS Supplemental Guidance: The organization develops an incident response plan that provides the organization with a roadmap for implementing its incident response capability; describes the structure and organization of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability within the organization; defines the resources and management support needed to effectively maintain and mature an incident response capability; and is reviewed and approved by designated officials within the organization; distributes copies of the incident response plan to all personnel with a role or responsibility for implementing the incident response plan; reviews the incident response plan at least annually (incorporating lessons learned from past incidents); revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and communicates incident response plan changes to all personnel with a role or responsibility for implementing the incident response plan, not later than 30 days after the change is made.

Applies to all Tiers

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented ICS maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the ICS maintenance policy and associated system maintenance controls.

Applies to all Tiers

MA-2 CONTROLLED MAINTENANCE

ICS Supplemental Guidance: The organization schedules, performs, documents, and reviews records of maintenance and repairs on ICS components in accordance with manufacturer or vendor specifications and/or organizational requirements; controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; requires that a designated official explicitly approve the removal of the ICS or system components from organizational facilities for off-site maintenance or repairs; sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Applies to all Tiers

MA-4 NON-LOCAL MAINTENANCE

ICS Supplemental Guidance: The organization authorizes, monitors, and controls non-local maintenance and diagnostic activities; allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the ICS; employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; maintains records for non-local maintenance and diagnostic activities; and terminates all sessions and network connections when non-local maintenance is completed.

Applies to all Tiers

MA-5 MAINTENANCE PERSONNEL

ICS Supplemental Guidance: The organization a establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and ensures that personnel performing maintenance on the ICS have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise ICS maintenance when maintenance personnel do not possess the required access authorizations. Federal employees and contractors that work on High Performance Green Buildings subject to the Federal Buildings Personnel Training Act will maintain their core competencies in www.fmi.gov.

Applies to all Tiers

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Applies to all Tiers

MP-2 MEDIA ACCESS

ICS Supplemental Guidance: The organization restricts access to ICS media which includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices, controller interfaces and programming devices) to the organization-

defined list of authorized individuals using organization-defined security measures. As-Built drawings, Building Information Models, and Construction-Operations Building information exchange data (if used) should be marked and treated as For Official Use Only (FOUO) at a minimum.

Applies to all Tiers

MP-6 MEDIA SANITIZATION

ICS Supplemental Guidance: The organization sanitizes ICS media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.

Applies to all Tiers

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Applies to all Tiers

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

ICS Supplemental Guidance: The organization develops and keeps current a list of personnel with authorized access to the facility where the ICS resides (except for those areas within the facility officially designated as publicly accessible); issues authorization credentials; reviews and approves the access list and authorization credentials every 90 days, removing from the access list personnel no longer requiring access.

Applies to Tiers 2d, 4a, and 5

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: The organization authorizes physical access to the facility where the ICS resides based on position or role.

PE-3 PHYSICAL ACCESS CONTROL

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to ICS facilities and assets to authorized individuals only. ICS are often constructed of

devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan.

Applies to Tiers 2d, 4a, and 5

References: NIST Special Publication 800-82

PE-6 MONITORING PHYSICAL ACCESS

ICS Supplemental Guidance: The organization monitors physical access to the ICS to detect and respond to physical security incidents; reviews physical access logs every 30 days; and coordinates results of reviews and investigations with the organization's incident response capability.

Applies to Tiers 4 and 5

PE-7 VISITOR CONTROL

ICS Supplemental Guidance: The organization controls physical access to the ICS by authenticating visitors before authorizing access to the facility where the ICS resides, other than areas designated as publicly accessible.

Applies to Tiers 2d, 4a, and 5

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: The organization escorts visitors and monitors visitor activity, when required.

PE-8 ACCESS RECORDS

ICS Supplemental Guidance: The organization maintains visitor access records to the facility where the ICS resides (except for those areas within the facility officially designated as publicly accessible) and reviews visitor access records every 30 days.

Applies to Tiers 2d, 4a, and 5

PE-12 EMERGENCY LIGHTING

ICS Supplemental Guidance: The organization employs and maintains automatic emergency lighting for the ICS that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Applies to all Tiers

PE-13 FIRE PROTECTION

ICS Supplemental Guidance: The organization employs and maintains fire suppression and detection devices/systems for the ICS that are supported by an independent energy source.

Applies to all Tiers

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

ICS Supplemental Guidance: The organization maintains temperature and humidity levels within the facility where the ICS resides at 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F; measured at the air intake inlet of the IT equipment casing and monitors temperature and humidity levels continuously.

Applies to Tiers 4a and 5

PE-15 WATER DAMAGE PROTECTION

ICS Supplemental Guidance: The organization protects the ICS from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Applies to Tiers 4a and 5

PE-16 DELIVERY AND REMOVAL

ICS Supplemental Guidance: The organization authorizes, monitors, and controls all system components entering and exiting the facility and maintains records of those items. ICS hardware, sensors and devices are typically maintained by contractor support and not always under the direct control of the organization.

Applies to Tiers 2d, 4a, 4b and 5

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Applies to all Tiers

PL-2 SYSTEM SECURITY PLAN

ICS Supplemental Guidance: The organization develops a security plan for the ICS that is consistent with the organization's enterprise architecture; explicitly defines the authorization boundary for the system; describes the operational context of the ICS in terms of missions and business processes; provides the security categorization of the ICS including supporting rationale; describes the operational environment for the ICS; describes relationships with or connections to other information systems; provides an overview of the security requirements for the system; describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and is reviewed and approved by the authorizing official or designated representative prior to plan implementation; reviews the security plan for the information, changes to the ICS/environment of operation or problems identified during plan implementation or security control assessments.

Applies to all Tiers

References: NIST Special Publication 800-82

PL-4 RULES OF BEHAVIOR

ICS Supplemental Guidance: The organization establishes the rules that describe their responsibilities and expected behavior with regard to information and ICS usage, makes them readily available to all ICS users, and receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the ICS.

Applies to all Tiers

PL-5 PRIVACY IMPACT ASSESSMENT

ICS Supplemental Guidance: The organization conducts a privacy impact assessment on the ICS in accordance with OMB policy. It is uncommon to have privacy information in an ICS, however, the vendor, contractor, and operator names can be used in conjunction with other phishing tools to build a comprehensive profile of systems users and the systems they support. OPSEC procedures should be used to mitigate exposure of critical information.

Applies to all Tiers

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Applies to all Tiers

PS-2 POSITION CATEGORIZATION

ICS Supplemental Guidance: The organization assigns a risk designation to all positions; establishes screening criteria for individuals filling those positions; and reviews and revises position risk designations annually.

Applies to all Tiers

PS-3 PERSONNEL SCREENING

ICS Supplemental Guidance: The organization screens individuals prior to authorizing access to the ICS; and rescreens individuals according applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position.

Applies to all Tiers

PS-4 PERSONNEL TERMINATION

ICS Supplemental Guidance: The organization, upon termination of individual employment, terminates ICS access, conducts exit interviews, retrieves all security-related organizational ICS-related property, and retains access to organizational information and ICS formerly controlled by terminated individual.

Applies to all Tiers

PS-5 PERSONNEL TRANSFER

ICS Supplemental Guidance: The organization reviews logical and physical access authorizations to ICS/facilities when personnel are reassigned or transferred to other positions within the organization and initiates actions to ensure all system accesses no longer required are removed within 24 hours.

Applies to all Tiers

PS-6 ACCESS AGREEMENTS

ICS Supplemental Guidance: The organization ensures that individuals requiring access to organizational information and the ICS sign appropriate access agreements prior to being granted access; and reviews/updates the access agreements annually or upon departure.

Applies to Tiers 2d, 4a, and 4b

PS-7 THIRD-PARTY PERSONNEL SECURITY

ICS Supplemental Guidance: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers; documents personnel security requirements; and monitors provider compliance.

Applies to all Tiers

PS-8 PERSONNEL SANCTIONS

ICS Supplemental Guidance: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Applies to all Tiers

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Applies to all Tiers

RA-2 SECURITY CATEGORIZATION

ICS Supplemental Guidance: The organization categorizes information and ICS in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; documents the security categorization results (including supporting rationale) in the security plan for the ICS; and ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative. Categorization must be closely coordinated with the Defense Critical Infrastructure Protection Plan, the USCYBERCOM Functional lead, and the OPSEC Functional lead.

Applies to all Tiers

References: NIST Special Publication 800-82

RA-3 RISK ASSESSMENT

ICS Supplemental Guidance: The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the ICS and the information it processes, stores, or transmits; documents risk assessment results in a risk assessment report; reviews risk assessment results at least annually; and updates the risk assessment at least

annually or whenever there are significant changes to the ICS or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Applies to all Tiers

References: NIST Special Publication 800-82

RA-5 VULNERABILITY SCANNING

ICS Supplemental Guidance: Vulnerability scanning and penetration testing are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken offline, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken offline for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the organization cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct scanning) in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a, 4b, 4n, and 5

References: NIST Special Publication 800-82

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Applies to all Tiers

SA-2 ALLOCATION OF RESOURCES

ICS Supplemental Guidance: The organization includes a determination of information security requirements for the ICS in mission/business process planning; determines, documents, and allocates the resources required to protect the ICS as part of its capital planning and investment control process; and establishes a discrete line item for information security in organizational programming and budgeting documentation. The ICS enclave must be entered into the DoD IT Portfolio Repository (DITPR) systems; budgetary breakouts for building level components, Real Property Installed Equipment,

and operations and maintenance must be closely coordinated by the IT and I&E communities and reflected in the IT, MILCON and SRM budgets.

Applies to all Tiers

SA-3 LIFE CYCLE SUPPORT

ICS Supplemental Guidance: The organization manages the ICS using a system development life cycle methodology that includes information security considerations; defines and documents ICS security roles and responsibilities throughout the system development life cycle; and identifies individuals having ICS security roles and responsibilities.

Applies to all Tiers

SA-4 ACQUISITIONS

ICS Supplemental Guidance: The SCADA/Control Systems Procurement Project provides example cyber security procurement language for ICS.

Applies to all Tiers

References: http://msisac.cisecurity.org/

SA-5 INFORMATION SYSTEM DOCUMENTATION

ICS Supplemental Guidance: The organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the ICS that describes: secure configuration, installation, and operation of the ICS; effective use and maintenance of security features/functions; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. The organization also obtains, protects as required, and makes available to authorized personnel, user documentation for the ICS that describes user-accessible security features/functions and how to effectively use those security features/functions; methods for user interaction with the ICS, which enables individuals to use the system in a more secure manner; and user responsibilities in maintaining the security of the information and ICS; and documents attempts to obtain ICS documentation when such documentation is either unavailable or nonexistent. Because ICSs can have a very long life, many vendors' user manuals are available online. As the firmware embedded default passwords cannot be changed, these legacy systems should be isolated as a compensating measure.

Applies to Tiers 2d, 4a, 4b and 5

SA-6 SOFTWARE USAGE RESTRICTIONS

ICS Supplemental Guidance: The organization: uses software and associated documentation in accordance with contract agreements and copyright laws; employs tracking systems for software and associated documentation protected by quantity

licenses to control copying and distribution; and controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Applies to all Tiers

SA-7 USER INSTALLED SOFTWARE

ICS Supplemental Guidance: The organization enforces explicit rules governing the installation of software by users.

Applies to all Tiers

SA-8 SECURITY ENGINEERING PRINCIPLES

ICS Supplemental Guidance: The organization applies ICS security engineering principles in the specification, design, development, implementation, and modification of the ICS. The Instrumentation, Systems, and Automation (ISA) 99 Committee (http://www.isa.org/isa99) has developed ANSI/ISA-99.02.01-2009, a standard that addresses the development and deployment of an ICS security program in detail.

Applies to Tiers 3, 4, and 5

References: NIST Special Publication 800-82

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

ICS Supplemental Guidance: The organization: requires that providers of external ICS services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; defines and documents government oversight and user roles and responsibilities with regard to external ICS services; and monitors security control compliance by external service providers.

Applies to Tiers 4a and 5

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Applies to all Tiers

SC-5 DENIAL OF SERVICE PROTECTION

ICS Supplemental Guidance: The ICS protects against or limits the effects of the following types of denial of service attacks: consumption of scarce, limited, or non-renewable resources; destruction or alteration of configuration information; physical destruction or alteration of network components.

Applies to Tier 5

SC-7 BOUNDARY PROTECTION

ICS Supplemental Guidance: The ICS monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Applies to Tiers 4a and 5

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: The organization limits the number of access points to the ICS to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

ICS Supplemental Guidance: The use of cryptography, including key management, is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The use of cryptographic key management in ICS is intended to support internal nonpublic use.

Applies to Tiers 2d, 4a, 4b and 5

SC-13 USE OF CRYPTOGRAPHY

ICS Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

Applies to Tiers 2d, 4a, 4b and 5

SC-14 PUBLIC ACCESS PROTECTIONS

ICS Supplemental Guidance: Generally, public access to ICS is not permitted.

Applies to all Tiers

SC-18 MOBILE CODE

ICS Supplemental Guidance: The organization defines acceptable and unacceptable mobile code and mobile code technologies; establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and authorizes, monitors, and controls the use of mobile code within the ICS. UFGS 25-10-10 restricts the mobile code the application software can require.

Applies to Tiers 2d, 4a, and 4b

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

Applies to Tiers 2, 3, 4, and 5

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The ICS, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services), enable verification of a chain of trust among parent and child domains.

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

ICS Supplemental Guidance: The organization develops, disseminates, and annually reviews/updates a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The organization also develops, disseminates, and annually reviews/updates formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Applies to all Tiers

SI-2 FLAW REMEDIATION

ICS Supplemental Guidance: The organization identifies and reports ICS flaws; tests software updates related to flaw remediation for effectiveness and potential side effects on organizational ICS before installation; and incorporates flaw remediation into the organizational configuration management process. Patching of software security flaws

must consider operational impact to control system; because the systems are always "on" it is often necessary to delay the implementation of a patch until the application software can be tested and/or patched.

Applies to Tiers 2d, 4a, 4b and 5

SI-3 MALICIOUS CODE PROTECTION

ICS Supplemental Guidance: The use of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

Applies to Tiers 2d, 4a, 4b and 5

SI-4 INFORMATION SYSTEM MONITORING

ICS Supplemental Guidance: The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ICS.

Applies to Tier 5 or at connection side of external network, may apply to Tiers 2d, 4a, and 4b

Control Enhancement: (6)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot prevent non-privileged users from circumventing intrusion detection and prevention capabilities, the organization employs appropriate compensating controls (e.g., enhanced auditing) in accordance with the general tailoring guidance.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

ICS Supplemental Guidance: The organization receives ICS security alerts, advisories, and directives from designated external organizations on an ongoing basis; generates internal security alerts, advisories, and directives as deemed necessary; disseminates security alerts, advisories, and directives to CNDSP Tier 1 for vetting. The CNDSP Tier 1 will pass the information to the accredited Tier 2 CNDSPs. Tier 2 CNDSPs are responsible for ensuring all Tier 3 entities receive the information. Tier 3 organizations will ensure all local Op Centers/LAN shops receive information; and implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. ICS vulnerabilities and patches are coordinated through the Department of Homeland Security (DHS) DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Applies to all Tiers

SI-9 INFORMATION INPUT RESTRICTIONS

ICS Supplemental Guidance: The organization restricts the capability to input information to the ICS to authorized personnel.

Applies to Tiers 2d, 4a, and 4b

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

ICS Supplemental Guidance: The organization handles and retains both information within and output from the ICS in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. In general, ICS do not output information other than audit and performance logs; the output is the continuous availability of the essential service being provided (i.e., power, water, HVAC, etc.). Reporting of performance and consumption data should be closely coordinated with the OPSEC Functional lead to ensure critical information is not divulged.

Applies to all Tiers

PM-1 INFORMATION SECURITY PROGRAM PLAN

ICS Supplemental Guidance: The organization develops and disseminates an organization-wide information security program plan that: provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; reviews the organization-wide ICS program plan annually; and revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

Applies to all Tiers

PM-2 SENIOR INFORMATION SECURITY OFFICER

ICS Supplemental Guidance: The organization appoints a senior ICS officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Applies to all Tiers

PM-3 INFORMATION SECURITY RESOURCES

ICS Supplemental Guidance: The organization ensures that all capital planning and investment requests include the resources needed to implement the ICS program and documents all exceptions to this requirement; employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and ensures that ICS resources are available for expenditure as planned. The I&E community will resource for the OT enclave listed in DITPR. Other inventory systems such as Computerized Maintenance Management Systems or Builder may be used for systems and subsystems detailed inventory. The I&E community must coordinate MILCON and SRM for Tier 4 and below and identify OT assets that will need technology refresh.

Applies to all Tiers

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

ICS Supplemental Guidance: The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational ICS are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

Applies to all Tiers

PM-5 INFORMATION SYSTEM INVENTORY

ICS Supplemental Guidance: The organization develops and maintains an inventory of its ICS. The I&E community will inventory and maintain all ICS systems to the sensor and actuator level using As-Built drawings, Building Information Models, Computerized Maintenance Management Systems, Builder, and Construction-Operations Building information exchange data (if used). The I&E and IT communities will identify the ICS enclave boundary and use this as the system of record identifier for DITPR.

Applies to all Tiers

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

ICS Supplemental Guidance: The organization develops, monitors, and reports on the results of information security measures of performance.

Applies to all Tiers

References: NIST Special Publication 800-55

PM-7 ENTERPRISE ARCHITECTURE

ICS Supplemental Guidance: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Applies to all Tiers

PM-9 RISK MANAGEMENT STRATEGY

ICS Supplemental Guidance: The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of ICS; and implements that strategy consistently across the organization. The strategy must be closely coordinated with the Defense Critical Infrastructure Protection Program, the USCYBERCOM and the OPSEC Functional leads.

Applies to all Tiers

PM-10 SECURITY AUTHORIZATION PROCESS

ICS Supplemental Guidance: The organization manages (i.e., documents, tracks, and reports) the security state of organizational ICS through security authorization processes; designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and fully integrates the security authorization processes into an organization-wide risk management program.

Applies to all Tiers

PM-11 MISSION/BUSINESS PROCESS DEFINITION

ICS Supplemental Guidance: The organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Applies to all Tiers

MODERATE IMPACT SYSTEMS

In addition to the Low Impact systems controls, the Moderate Impact system includes the additional following controls:

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The ICS automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Applies to Tiers 2d, 4a, and 4b

AC-10 CONCURRENT SESSION CONTROL

ICS Supplemental Guidance: In situations where the ICS cannot support concurrent session control, the organization employs appropriate compensating controls (e.g., providing increased auditing measures) in accordance with the general tailoring guidance.

Applies to Tiers 3 and 4

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.

Applies to Tiers 4a and 4b

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The ICS integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Applies to Tiers 2d, 4a, and 4b

AU-7 AUDIT REDUCTION AND REPORT GENERATION

ICS Supplemental Guidance: In general, audit reduction and report generation is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including audit reduction and report generation, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a, and 4b

AU-9 PROTECTION OF AUDIT INFORMATION

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The ICS backs up audit records weekly onto a different system or media than the system being audited.

Applies to Tiers 2d, 4a, and 4b

CM-3 CONFIGURATION CHANGE CONTROL

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization tests, validates, and documents changes to the ICS before implementing the changes on the operational system.

Applies to Tiers 2d, 3, 4 and 5

CM-4 SECURITY IMPACT ANALYSIS

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Applies to Tiers 4a and 5

CM-6 CONFIGURATION SETTINGS

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, the organization employs non-automated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Applies to Tiers 2d, 3, 4a, 4b, and 5

CM-7 LEAST FUNCTIONALITY

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot employ automated mechanisms to prevent program execution, the organization employs compensating controls (e.g., external automated mechanisms, procedures) in accordance with the general tailoring guidance.

Applies to all Tiers

CP-2 CONTINGENCY PLAN

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization coordinates contingency plan development with organizational elements responsible for related plans.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: The organization plans for the resumption of essential missions and business functions within 12 hours (Availability Moderate), as defined in the contingency plan of contingency plan activation.

Control Enhancements: (4)

ICS Enhancement Supplemental Guidance: The organization plans for the full resumption of missions and business functions within 1-5 days (Availability Moderate), as defined in the contingency plan of contingency plan activation.

Applies to all Tiers

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

Applies to all Tiers

CP-8 TELECOMMUNICATIONS SERVICES

ICS Supplemental Guidance: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of ICS operations for essential missions and business functions within 1 hour for High Availability and 12 hours for Moderate Availability systems when the primary telecommunications capabilities are unavailable.

Applies to Tiers 4 and 5

CP-9 INFORMATION SYSTEM BACKUP

Control Enhancements: (5)

ICS Enhancement Supplemental Guidance: The organization transfers ICS backup information to the alternate storage site 24 hour (Availability Moderate) as defined in the contingency plan.

Applies to Tiers 2d and 4a

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support multifactor authentication, the organization employs compensating controls in accordance with the general tailoring guidance (e.g., implementing physical security measures).

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support multifactor authentication, the organization employs compensating controls in accordance with the general tailoring guidance (e.g., implementing physical security measures).

Control Enhancements: (4)

ICS Enhancement Supplemental Guidance: The ICS uses multifactor authentication for local access to non-privileged accounts.

Control Enhancements: (9)

ICS Enhancement Supplemental Guidance: The ICS uses replay-resistant authentication mechanisms (e.g. Time Stamp Cryptographic mechanisms, Protected incremented Counters, Nonces, Cnonce) for network access to non-privileged accounts.

Applies to Tiers 2d, 4a, and 4b

MA-6 TIMELY MAINTENANCE

ICS Supplemental Guidance: The organization obtains maintenance support and/or spare parts for security-critical ICS components and/or key information technology components within 12 hours of failure (Availability Moderate).

Applies to all Tiers

MP-2 MEDIA ACCESS

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The ICS uses cryptographic mechanisms to protect and restrict access to information on portable digital media.

Applies to all Tiers

MP-5 MEDIA TRANSPORT

Control Enhancements: (4)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support cryptographic mechanisms, the organization employs compensating controls in accordance with the general tailoring guidance (e.g., implementing physical security measures).

Applies to all Tiers

MP-6 MEDIA SANITIZATION

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization tracks, documents, and verifies media sanitization and disposal actions.

Applies to all Tiers

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

ICS Supplemental Guidance: The organization controls physical access to ICS distribution and transmission lines within organizational facilities.

Applies to Tiers 2d, 4a, and 5

PE-6 MONITORING PHYSICAL ACCESS

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization monitors real-time physical intrusion alarms and surveillance equipment.

Applies to Tiers 4 and 5

PE-11 EMERGENCY POWER

ICS Supplemental Guidance: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the ICS in the event of a primary power source loss.

Applies to Tiers 2, 3, and 4

PE-12 EMERGENCY LIGHTING

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.

Applies to all Tiers

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the ICS.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Applies to Tiers 4a and 5

PE-17 ALTERNATE WORK SITE

ICS Supplemental Guidance: The organization employs:

1. Temperature, noise, ventilation and light levels adequate for maintaining a normal level of job performance.
2. Stairs with four or more steps must be equipped with handrails.
3. Circuit breakers or fuses in the electrical panel are labeled as to the intended service.
4. All electrical equipment must be free of recognized hazards that would cause physical harm (e.g., loose or frayed wires).
5. The building's electrical system will permit the grounding of electrical equipment. Aisles, doorways, and corners are free of obstructions to permit visibility and movement. File cabinets and storage closets arranged so drawers and doors do not open into walkways.
6. Phone lines, electrical cords, and extension wires are secured under a desk or alongside a baseboard.
7. The office space must be neat, clean, and free of excess amounts of combustibles. Sufficient light for reading at alternate work sites; assesses as feasible, the effectiveness of security controls at alternate work sites; and provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Applies to all Tiers

SA-4 ACQUISITIONS

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the ICS, ICS components, or ICS services in sufficient detail to permit analysis and testing of the controls.

Applies to all Tiers

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the ICS in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Applies to Tiers 2d, 4a, 4b and 5

SC-5 DENIAL OF SERVICE PROTECTION

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The ICS manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

Applies to Tier 5

SC-8 TRANSMISSION INTEGRITY

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function). Each mechanism has a different delay impact.

Applies to Tiers 2d, 4a, 4b and 5

SC-13 USE OF CRYPTOGRAPHY

Control Enhancements: (4)

ICS Enhancement Supplemental Guidance: The organization employs NIST FIPS-Validated Unclassified systems, NSA Approved/FIPS-Validated for Classified systems cryptography to implement digital signatures.

Applies to Tiers 2d, 4a, 4b and 5

SI-2 FLAW REMEDIATION

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to conduct and report on the status of flaw remediation, the organization employs non-automated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a, 4b and 5

HIGH IMPACT SYSTEMS

In addition to the Low and Moderate Impact systems controls, the High Impact system includes the additional following controls:

AU-9 PROTECTION OF AUDIT INFORMATION

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: The ICS uses cryptographic mechanisms to protect the integrity of audit information and audit tools.

Applies to Tiers 2d, 4a, and 4b

AU-12 AUDIT GENERATION

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICScannot support the use of automated mechanisms to generate audit records, the organization employs non-automated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Applies to Tiers 2d, 4a, and 4b (0)

CA-2 SECURITY ASSESSMENTS

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization includes as part of security control assessments, annually or more frequently as required by the security plan, for announced in-depth monitoring; malicious user testing; penetration testing; red team exercises; and/or other forms of security testing (e.g. vulnerability scans, integrity checks, security readiness reviews) as necessary.

Applies to all Tiers

CM-3 CONFIGURATION CHANGE CONTROL

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization employs automated mechanisms to document proposed changes to the ICS; notify designated approval authorities; highlight approvals that have not been received by 7 days; inhibit change until designated approvals are received; and document completed changes to the ICS.

Applies to Tiers 2d, 3, 4, and 5

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot prevent the installation of software programs that are not signed with an organizationally-recognized and approved certificate, the organization employs alternative mechanisms or procedures as compensating controls (e.g., auditing of software installation) in accordance with the general tailoring guidance.

Applies to Tiers 2d, 3, 4a, 4b, and 5

CM-6 CONFIGURATION SETTINGS

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization employs automated mechanisms to respond to unauthorized changes to configuration settings.

Applies to Tiers 2d, 3, 4a, 4b, and 5

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of ICS components.

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: The organization employs automated mechanisms continuously to detect the addition of unauthorized components/devices into the ICS; and disables network access by such components/devices or notifies designated organizational officials.

Applies to Tiers 2d, 3, and 4

CP-2 CONTINGENCY PLAN

Control Enhancements: (5)

ICS Enhancement Supplemental Guidance: The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full ICS restoration at primary processing and/or storage sites.

Control Enhancements: (6)

ICS Enhancement Supplemental Guidance: The organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.

Applies to all Tiers

CP-3 CONTINGENCY TRAINING

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Applies to all Tiers

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

Applies to all Tiers

CP-8 TELECOMMUNICATIONS SERVICES

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.

Control Enhancements: (4)

ICS Enhancement Supplemental Guidance: The organization requires primary and alternate telecommunications service providers to have contingency plans.

Applies to Tier 5

CP-9 INFORMATION SYSTEM BACKUP

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization uses a sample of backup information in the restoration of ICS functions as part of contingency plan testing.

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: The organization stores backup copies of the operating system and other critical ICS software, as well as copies of the ICS inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

Applies to Tiers 2d and 4a

IR-2 INCIDENT RESPONSE TRAINING

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization employs automated mechanisms to provide a more thorough and realistic training environment.

Applies to Tiers 4a and 5

IR-5 INCIDENT MONITORING

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Applies to Tiers 2d, 4a, and 4b

MA-2 CONTROLLED MAINTENANCE

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

Applies to all Tiers

MP-4 MEDIA STORAGE

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization employs cryptographic mechanisms to protect information in storage.

Applies to all Tiers

PE-3 PHYSICAL ACCESS CONTROL

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization enforces physical access authorizations to the ICS independent of the physical access controls for the facility.

Control Enhancements: (4)

ICS Enhancement Supplemental Guidance: The organization uses lockable physical casings to protect the ICS from unauthorized physical access.

Control Enhancements: (6)

ICS Enhancement Supplemental Guidance: The organization employs a penetration testing process that includes annual unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

Applies to Tiers 2d, 4a, and 5

PE-8 ACCESS RECORDS

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization maintains a record of all physical access, both visitor and authorized individuals.

Applies to Tiers 2d, 4a, and 5

PE-11 EMERGENCY POWER

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization provides a long-term alternate power supply for the ICS that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization provides a long-term alternate power supply for the ICS that is self-contained and not reliant on external power generation.

Applies to Tiers 2, 3, and 4

PE-13 FIRE PROTECTION

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization employs fire detection devices/systems for the ICS that activate automatically and notify the organization and emergency responders in the event of a fire.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization employs fire suppression devices/systems for the ICS that provide automatic notification of any activation to the organization and emergency responders.

Control Enhancements: (3)

ICS Enhancement Supplemental Guidance: The organization employs an automatic fire suppression capability for the ICS when the facility is not staffed on a continuous basis.

Control Enhancements: (4)

ICS Enhancement Supplemental Guidance: The organization ensures that the facility undergoes annual fire marshal inspections and promptly resolves identified deficiencies.

Applies to all Tiers

RA-5 VULNERABILITY SCANNING

Control Enhancements: (9)

ICS Enhancement Supplemental Guidance: The organization employs an independent penetration agent or penetration team to conduct a vulnerability analysis on the ICS; and perform penetration testing on the ICS based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.

Applies to Tiers 2d, 4a, 4b, 4n and 5

SA-4 ACQUISITIONS

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the ICS, ICS components, or ICS services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.

Applies to all Tiers

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control Enhancements: (4)

ICS Enhancement Supplemental Guidance: The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of ICS in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Applies to Tiers 2d, 4a, 4b and 5

SA-11 DEVELOPER SECURITY TESTING

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization requires that ICS developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization requires that ICS developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.

Applies to all Tiers

SC-3 SECURITY FUNCTION ISOLATION

ICS Supplemental Guidance: In situations where the ICS cannot support security function isolation, the organization employs compensating controls (e.g., providing increased auditing measures, limiting network connectivity) in accordance with the general tailoring guidance.

Applies to Tiers 3, 4, and 5

SC-6 RESOURCE PRIORITY

ICS Supplemental Guidance: The ICS limits the use of resources by priority.

Applies to all Tiers

SC-28 PROTECTION OF INFORMATION AT REST

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.

Applies to Tiers 3, 4, and 5

SC-33 TRANSMISSION PREPARATION INTEGRITY

ICS Supplemental Guidance: The ICS protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.

Applies to Tiers 3, 4, and 5

SI-7 SOFTWARE AND INFORMATION INTEGRITY

ICS Supplemental Guidance: The ICS detects unauthorized changes to software and information.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization reassesses the integrity of software and information by performing annually or changes in accordance with guidance/direction from an authoritative source or USCYBERCOM tactical orders/directives integrity scans of the ICS.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

Applies to Tiers 3, 4, and 5

SI-13 PREDICTABLE FAILURE PREVENTION

ICS Supplemental Guidance: The organization protects the ICS from harm by considering mean time to failure for any component within a system requiring high availability in specific environments of operation; and provides substitute ICS components, when needed, and a mechanism to exchange active and standby roles of the components.

Applies to Tiers 3, 4, and 5

6. Specific Value Parameters

Table 4: Values for Parameters

CONTROL	ICS OVERLAY
IA-5 (1)	Passwords may be non-changeable; embedded firmware by vendor

7. Regulatory/Statutory Controls

Table 5: Regulatory/Statutory Security Controls

CONTROL	ICSs
PE-13 Fire Protection	Reference: National Electric Code (NFPA 70) Reference: National Fire Code (NFPA 1)
PE-12 Emergency Lighting	Reference: National Electric Code (NFPA 70) Reference: National Fire Code (NFPA 1)
PE-14 Temperature and Humidity Controls	Reference: National Electric Code (NFPA 70) Reference: National Fire Code (NFPA 1)
PE-15 Water Damage Protection	Reference: National Electric Code (NFPA 70) Reference: National Fire Code (NFPA 1)

8. Tailoring Considerations

When tailoring a security control set that includes the ICS Overlay, care should be taken that regulatory/statutory security controls are not tailored out of the control set. These security controls are required to satisfy the regulatory/statutory requirements of the Energy Performance ACT 2005, Energy Independence Security Act 2007, and Fiscal Year 2010 National Defense Authorization Act.

9. Duration

The overlay should be evaluated for revision when government or industry issues new guidance that may impact designation of ICS related security controls.

10. Definitions

Alternative Fuel Vehicle (AFV)	An AFV is a vehicle that runs on a fuel other than "traditional" petroleum fuels (petrol or diesel); and also refers to any technology of powering an engine that does not involve solely petroleum (e.g. electric car, hybrid electric vehicles, solar powered).
Advanced Metering Infrastructure (AMI)	Advanced metering systems are comprised of state-of-the-art electronic/digital hardware and software, which combine interval data measurement with continuously available remote communications. These systems enable measurement of detailed, time-based information and frequent collection and transmittal of such information to various parties. AMI typically refers to the full measurement and collection system that includes meters at the customer site, communication networks between the customer and a service provider, such as an electric, gas, or water utility, and data reception and management systems
BACnet	The term BACnet is used in two ways. First meaning the BACnet Protocol Standard - the communication requirements as defined by ASHRAE-135 including all annexes and addenda. The second to refer to the overall technology related to the ASHRAE-135 protocol.
Building Automation System (BAS)	A BAS is a distributed control system. The control system is a computerized, intelligent network of electronic devices designed to monitor and control the mechanical electronics, and lighting systems in a building. BAS core functionality keeps the building climate within a specified range, provides lighting based on an occupancy schedule, and monitors system performance and device failures and provides email and/or text notifications to building engineering or maintenance staff. The BAS functionality reduces building energy and maintenance costs when compared to a non-controlled building. A building controlled by a BAS is often

	referred to as an intelligent building or a smart home.
Building Control System (BCS)	A control system for building electrical and mechanical systems, typically HVAC (including central plants) and lighting. A building control system is one type of a Field Control System.
Building Control Network (BCN)	The network used by the Building Control System. Typically the BCN is a BACnet ASHRAE-135 or LonWorks CEA-709.1-C network installed by the building control system contractor.
Cyber-physical systems (CPS)	CPS are engineered systems that are built from and depend upon the synergy of computational and physical components. Emerging CPS will be coordinated, distributed, and connected, and must be robust and responsive. The CPS of tomorrow will need to far exceed the systems of today in capability, adaptability, resiliency, safety, security, and usability. Examples of the many CPS application areas include the smart electric grid, smart transportation, smart buildings, smart medical technologies, next-generation air traffic management, and advanced manufacturing.
Data Historian	A centralized database supporting data analysis using statistical process control techniques.
Defense Critical Infrastructure Protection (DCIP)	A program with the DoD to evaluate, monitor, and risk rank mission critical infrastructure assets.
Direct Digital Control (DDC)	Control consisting of microprocessor-based controls with the control logic performed by software.
Electronic Security Systems (ESS)	Electronic Security Systems are operations systems that provide monitoring and alarming through the combination of hardware, software, firmware, and devices to enhance the efficiency and effectiveness of a physical security program. ESS use exterior and interior sensors and other terminal devices to provide asset protection through physical and operational security of a geographic area, building, or area within a building. ESS

	includes access control systems, perimeter monitoring systems, intrusion detection systems, video management and analytic systems, physical security information management systems, and land mobile radios. The various systems may be integrated at the Security Operations Center or may be stand-alone.
Emergency Management Information Systems (EMIS)	EMIS are used for continuity and interoperability between emergency management stakeholders and supports the emergency management process by providing an infrastructure that integrates emergency plans at all levels of government and non-government involvement, and by utilizing the management of all related resources (including human and other resources) for all four phases of emergencies. The system must meet requirements established by the National Incident Management System and typically includes an incident management tracking capability, a geospatial common operating picture, and the radio and telecommunications network for first responders. EMIS are often integrated with local government First Alert and the police/fire CAD 911 systems.
Enclave	Enclaves provide standard cybersecurity capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.
Energy Service Interface (ESI)	A network-centric device and gateway. It provides security, and often, coordination functions that enable secure interactions between network devices and the electric power company. It may permit applications such as remote load control, monitoring and control of distributed generation, display of customer usage, reading of non-energy meters, and integration with building management

	systems. It also provides auditing/logging functions that record transactions to and from networking devices.
Exterior Lighting and Messaging Systems	Exterior lighting systems and messaging systems use a variety of control systems, with a mix of legacy analog and newer digital capabilities. Lights can be controlled with sensors and remote services. There are several types of exterior lights: street lights are used to light roadways and walkways at night. LED and photovoltaic luminaires to provide energy-efficient alternative to traditional street light fixtures; Floodlights are used to illuminate outdoor playing fields or work zones during nighttime; floodlights can be used to illuminate outdoor playing fields or work zones during nighttime hours; beacon lights are positioned at the intersection of two roads to aid in navigation; security lights can be used along roadways in urban areas, or behind homes or commercial facilities; entry lights can be used outside to illuminate and signal the entrance to a property. These lights are installed for safety, security, and for decoration. Message boards are used to control vehicle and pedestrian traffic, as scrolling information at property and building entrances, and at transit nodes to display arrival and departure times. Message boards can be LED, plasma, or light bulb displays.
Facility Point of Connection (FPOC)	The FPOC is the point of connection between the UMCS network backbone (an IP network) and the field control network (either an IP network or a non-IP network). The hardware at this location which provides the connection is referred to as the FPOC Hardware. FPOC hardware takes the form of a control protocol router, a control protocol gateway, or an IP device such as a switch or firewall. In general, the term "FPOC Location" means the place where this connection occurs, and "FPOC Hardware" means the device that provides the connection. Sometimes the term "FPOC" is used to mean either and its actual meaning (i.e. location or hardware) is determined by the

	context in which it is used.
Federal Real Property Profile (FRPP)	A common data dictionary and system used by the federal government to create a unique Real Property Unique Identifier (RPUID) for owned and leased properties.
Field Control Network	The network used by a field control system.
Field Control System (FCS)	A building control system or Utility Control System (UCS).
Field Device	Control equipment (controller, sensor, actuator etc) that is connected to/part of a field control system.
Fire Alarm and Life Safety Systems	A fire alarm system consists of components and circuits arranged to monitor and annunciate the status of fire alarm or supervisory signal initiating devices and to initiate the appropriate response to those signals. Fire systems include the sprinklers, sensors, panels, exhaust fans, signage, and emergency backup power required for building protection and occupant emergency egress. Life safety systems enhance or facilitate evacuation smoke control, compartmentalization, and/or isolation.
Human-Machine Interface (HMI)	The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to aPC with a color graphics display running dedicated HMI software.
Industrial Control System (ICS)	A system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems includes supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.
Installation Processing Node	A fixed DoD data center serving a single DoD installation with local services that cannot be (technically or economically) provided from a

	Core Data Center (CDC). There will only be one IPN per DoD installation but each IPN may have multiple enclaves to accommodate unique installation needs (e.g. Joint Bases). IPNs will connect to the CDCs.
Intelligent Transportation Systems (ITS)	ITS are systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport. Intelligent transport technologies include, wireless communications, computational technologies, floating car data/floating cellular data, sensing technologies, inductive loop detection, video vehicle detection, and Bluetooth detection. Intelligent transport applications include emergency vehicle notification systems, automatic road enforcement, variable speed limits, collision avoidance systems, and dynamic traffic light sequence.
Land Mobile Radios (LMR)	Land mobile radios are IP-based P25 equipment used by security, first responders and emergency managers to communicate over a secure channel for day to day operations and public safety events. LMR's and the P25 network interconnect transmission sites, management systems, dispatch console systems, logging recorders and data networks. The system operates in the Department of Defense UHF spectrum in the 380–399.9MHz frequency range.
Java Application Control Engine (JACE)	JACE is a mechanism to connect individual building control systems via a real time common objects model.
LonTalk®	A networking protocol developed by Echelon Corporation and recognized by ANSI/CEA as ANSI/CEA-709.1-C. LonTalk implements layers 1-6 of the OSI reference model.
LonWorks®	A networking platform (created by Echelon Corporation) that provides solutions to numerous problems of designing, building, installing, and maintaining control networks.
Meter Data Management System (MDMS)	A system which automatically and reliably collects regular interval energy use data, processes the data to create meaningful information, and distributes to energy

	stakeholders who can take action to reduce energy use.
Military Construction (MILCON)	MILCON appropriations are defined in 10 U.S.C. 2801, and includes construction, development, conversion, or extension of any kind carried out with respect to a military installation. MILCON includes construction projects for all types of buildings, roads, airfield pavements, and utility systems.
Modbus	A basic protocol for control network communications generally used in SCADA systems. The Modbus protocol definition is maintained by The Modbus Organization.
Monitoring and Control (M&C) Software	The UMCS 'front end' software which performs supervisory functions such as alarm handling, scheduling and data logging and provides a user interface for monitoring the system and configuring these functions.
Net Zero Energy	A Net Zero Energy Installation (NZEI) is an installation that produces as much energy on site as it uses, over the course of a year.
Net Zero Water	A Net Zero Water Installation limits the consumption of freshwater resources and returns water back to the same watershed so not to deplete the groundwater and surface water resources of that region in quantity and quality over the course of a year.
Net Zero Waste	A net zero waste installation is an installation that reduces, reuses, and recovers waste streams, converting them to resource values with zero landfill over the course of a year.
OPC Data Access	This group of standards provides specifications for communicating real-time data from data acquisition devices to display and interface devices like Human-Machine Interfaces (HMI). The specifications focus on the continuous communication of data.

Operations and Maintenance (O&M)	O&M appropriations are used to finance "expenses" not related to military personnel or RDT&E. Types of expenses funded by O&M include DoD civilian salaries, supplies and materials, maintenance of equipment, certain equipment items, real property maintenance, rental of equipment and facilities, food, clothing, and fuel.
Operational Technologies (OT)	OT is physical-equipment-oriented technology and systems that deal with the actual running of plants and equipment, devices to ensure physical system integrity and to meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software.
Physical Access Control System (PACs)	PACS are required by HSPD-12 and the basic components of a PACs are the head-end server, panels, door controllers, readers, lock or strike mechanisms and the user identity cards.
Platform Information Technology (PIT)	PIT are IT or OT resources, both hardware and software, and include: weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems to include supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks).

Platform Information Technology Interconnect (PITI)	PITI is a term used in the current DIACAP process, but will be sunset with the new RMF process. The PITI is where a physical or logical connection at or crossing the boundary between a Platform IT system and a non-Platform IT.
Programmable Logic Controller (PLC)	A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing.
Research, Development, Test and Evaluation (RDT&E)	RDT&E appropriations finance research, development, test and evaluation efforts performed by contractors and government installations to develop equipment, material, or computer application software; its development, test and evaluation, and its initial operational test and evaluation.
Safety Instrumented System (SIS)	A system that is composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined conditions are violated. Other terms commonly used include emergency shutdown system (ESS), safety shutdown system (SSD), and safety interlock system (SIS).
Special Purpose Processing Node	A fixed data center supporting special purpose functions that cannot (technically or economically) be supported by CDCs or IPNs due to its association with mission specific infrastructure or equipment (e.g., communications and networking, manufacturing, training, education, meteorology, medical, modeling & simulation, test ranges, etc.). No general purpose processing or general purpose storage can be provided by or through a SPPN. SPPNs will connect to the CDCs via IPNs.

Supervisory Control and Data Acquisition (SCADA)	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.
Sustainment, Restoration and Modernization (SRM)	Sustainment means the maintenance and repair activities necessary to keep and inventory of facilities in good working order. Restoration means the restoration of real property to such a condition that it may be used for its designated purpose. Modernization means the alteration or replacement of facilities solely to implement new or higher standards, to accommodate new functions, or to replace building components that typically last more than 50 years.
TP/FT-10 (LonWorks)	A Free Topology Twisted Pair network (at 78 kbps) defined by CEA-709.3. This is the most common media type for a CEA-709.1-C control network.
TP/XF-1250 (LonWorks)	A high speed (1.25 Mbps) twisted pair, doubly-terminated bus network defined by the LonMark Interoperability Guidelines. This media is typically used only as a backbone media to connect multiple TP/FT-10 networks.
UMCS Network	An IP network connecting multiple field control systems to the Monitoring and Control Software using one or more of: LonWorks (CEA-709.1-C and CEA-852-B), BACnet ASHRAE-135 Annex J), Modbus or OPC DA.

ATTACHMENT 4 CSET 5.1 INSTALLATION ICS ENCLAVE EXAMPLE