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).

Industrial Control Systems Overlay

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.

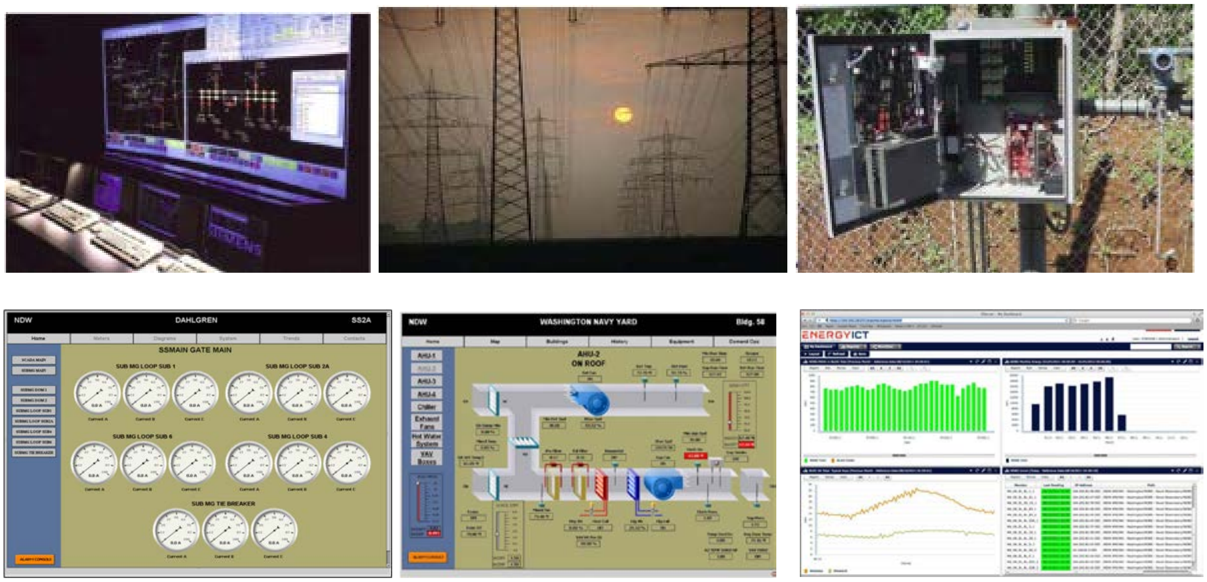


Figure 1 – ICS Human Machine Interface, System, Remote Terminal Unit[1]

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, 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

[1] 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.

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.

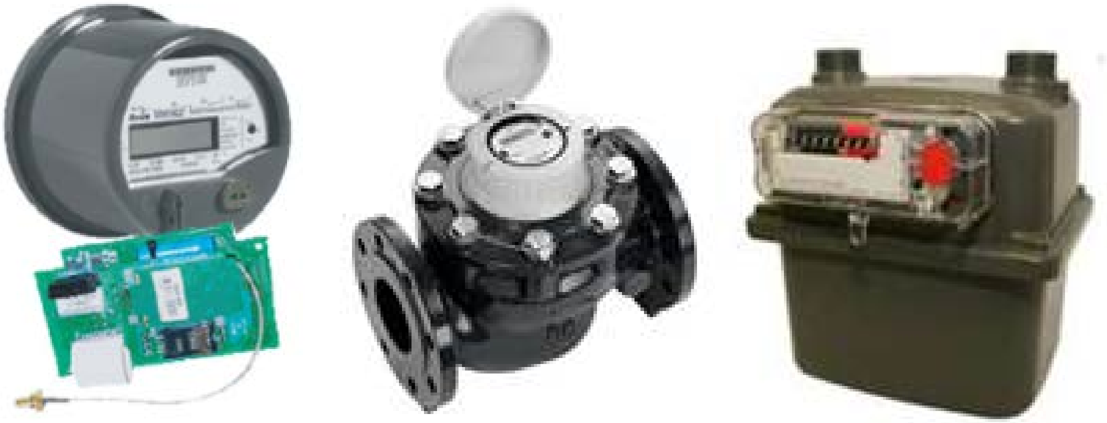


Figure 2 – Advanced Meter Infrastructure (Smart Meters) for Electric, Water, Gas

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.

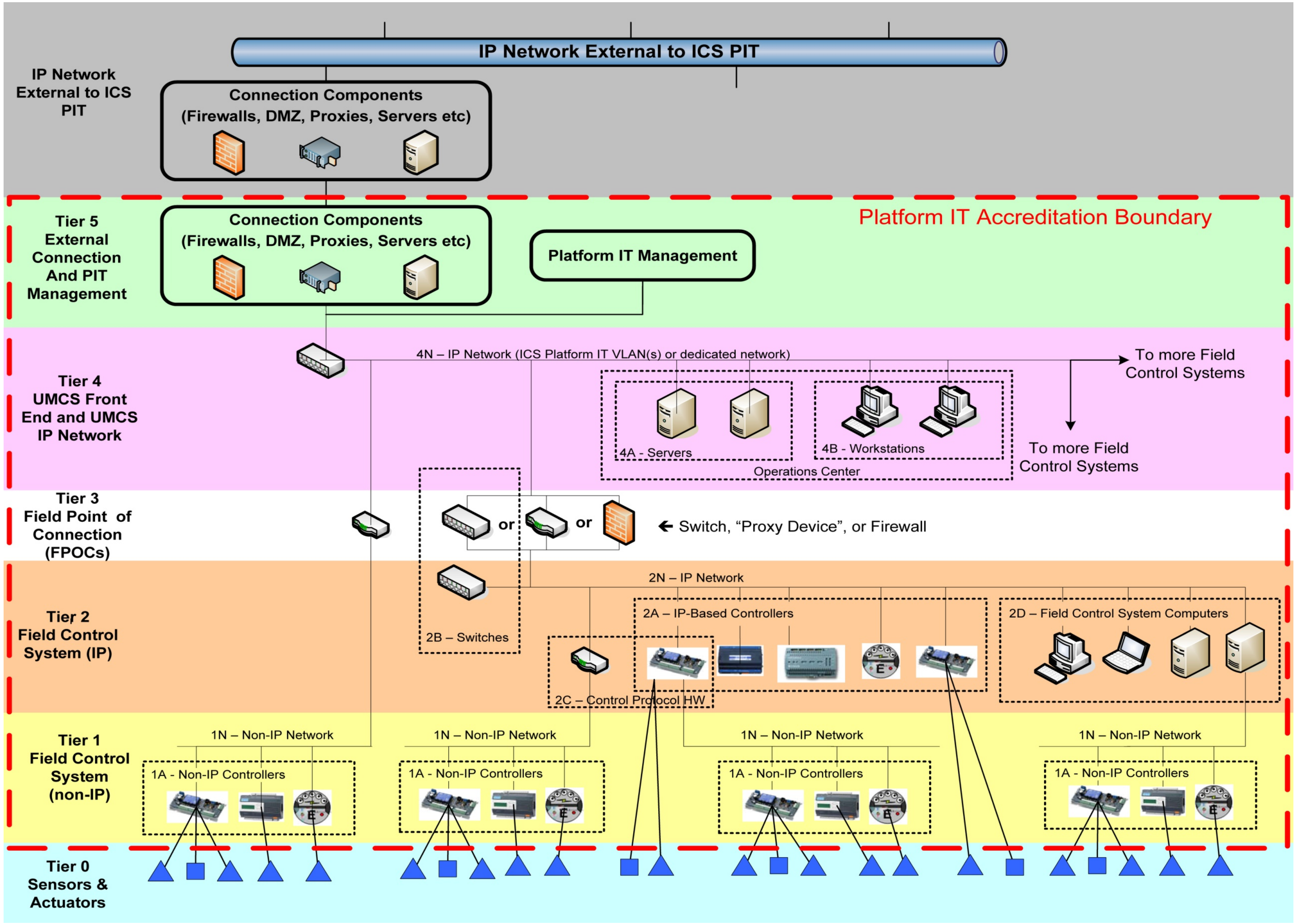
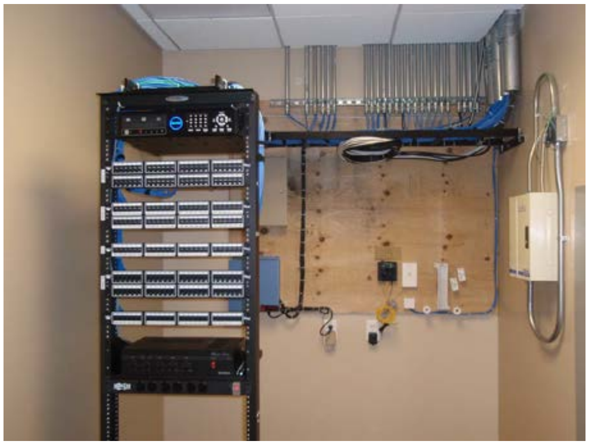

IP Network External to ICS PIT
IP Network External to ICS PIT
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Platform IT Accreditation Boundary
Tier 5 External Connection And PIT Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Platform IT Management
Tier 4 UMCS Front End and UMCS IP Network
4N – IP Network (ICS Platform IT VLAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
Operations Center
To more Field Control Systems
Tier 3 Field Point of Connection (FPOCs)
or
or
Switch, "Proxy Device", or Firewall
Tier 2 Field Control System (IP)
2N – IP Network
2A – IP-Based Controllers
2D – Field Control System Computers
2B – Switches
2C – Control Protocol HW
Tier 1 Field Control System (non-IP)
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
1N – Non-IP Network
1A - Non-IP Controllers
Tier 0 Sensors & Actuators

Figure 3 – ICS Tiers

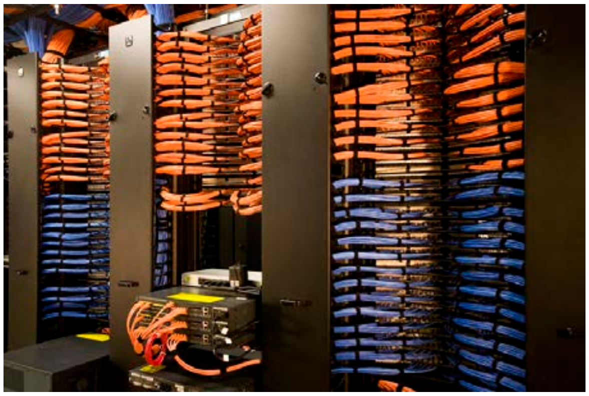
The ICS tier architecture is used to define the accrediation boundary for OT systems and is a logical representation of the OT network. The actual physical system can span many miles; for example, locks and dams, pipelines, electric transmission and distribution systems can have many non-contiguous components, 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:



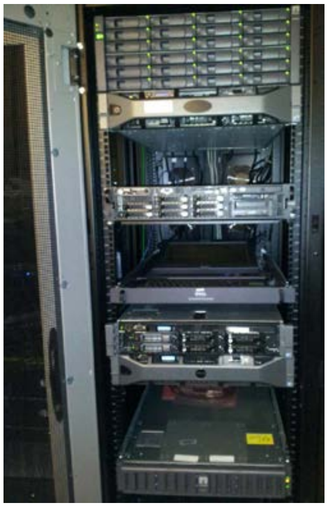
5: A Tier 5 Demarcation Point or Main Point of Presence where the external meets the internal interface.



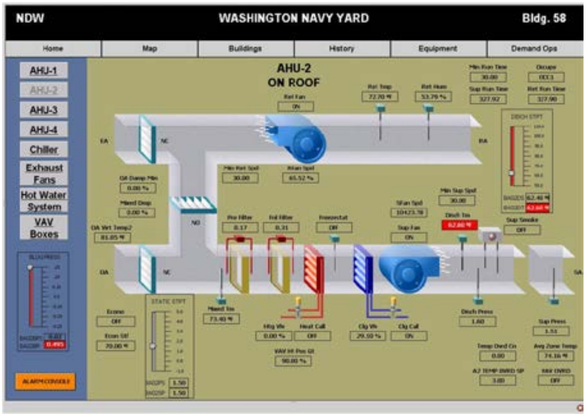
5: A Tier 5 IT rack and servers located in an Installation Processing Node.

.

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

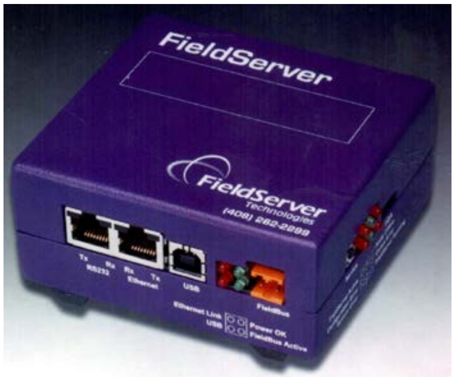


4-A: A Tier 4 OT rack and servers located in an Energy Operations Center, Special Purpose Processing Node.

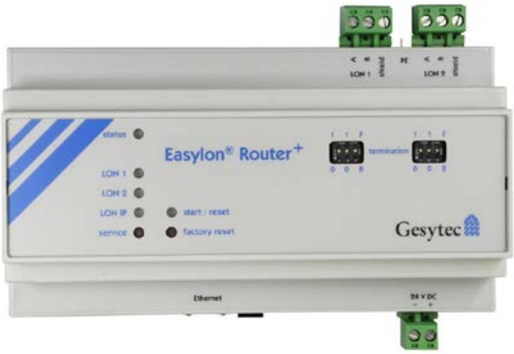


4-B: Workstation or wall display of HMI for the UMCS.

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

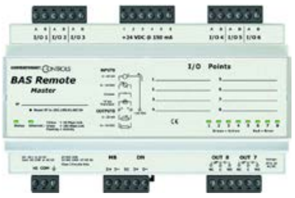


3-FS: A Tier 3 FPOC gateway (application layer proxy). The Tier 4 network is Modbus over IP over 10/100 Mbps Ethernet. The Tier 1 network is proprietary over proprietary 2-wire media. Note this is the same device as in 2C-FS.



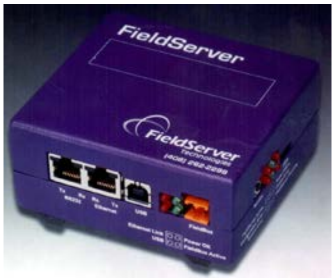
3-LIP: A Tier 3 FPOC router between 3 LonTalk networks: Tier 1 Lon over TP/FT-10, Tier 1 Lon over TP/FT-10, and Tier 4 Lon over IP over Ethernet.

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



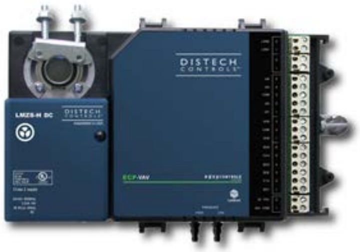
2A-CC: Very basic Tier 2A controller capable of monitoring six analog inputs and reporting their values to the network and setting two outputs. Network is BACnet over IP over 10/100 Mbps.

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.

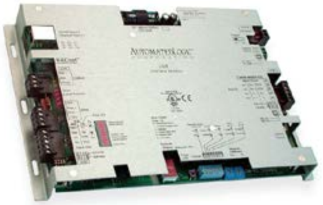


2C-FS: A Tier 2C gateway (application layer proxy). The Tier 2 network is Modbus over IP over 10/100 Mbps Ethernet. The Tier 1 network is proprietary over proprietary 2-wire media.

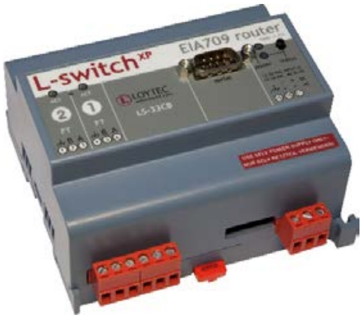
Figure 7 – Tier 2: IP portion of the Field Control System



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.

3 **Facility Points of Connection (FPOCs)**	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). 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.*	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). 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:** o Major air handling unit (AHU) controller, o Supervisory Controller o Electric meter (IP) • **Tier 2B:** o "Dumb" Ethernet switch • **Tier 2C:** o BACnet MS/TP to BACnet/IP router o Gateway between non-standard, non-IP protocol and a standard control protocol over IP • **Tier 2D:** o 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.

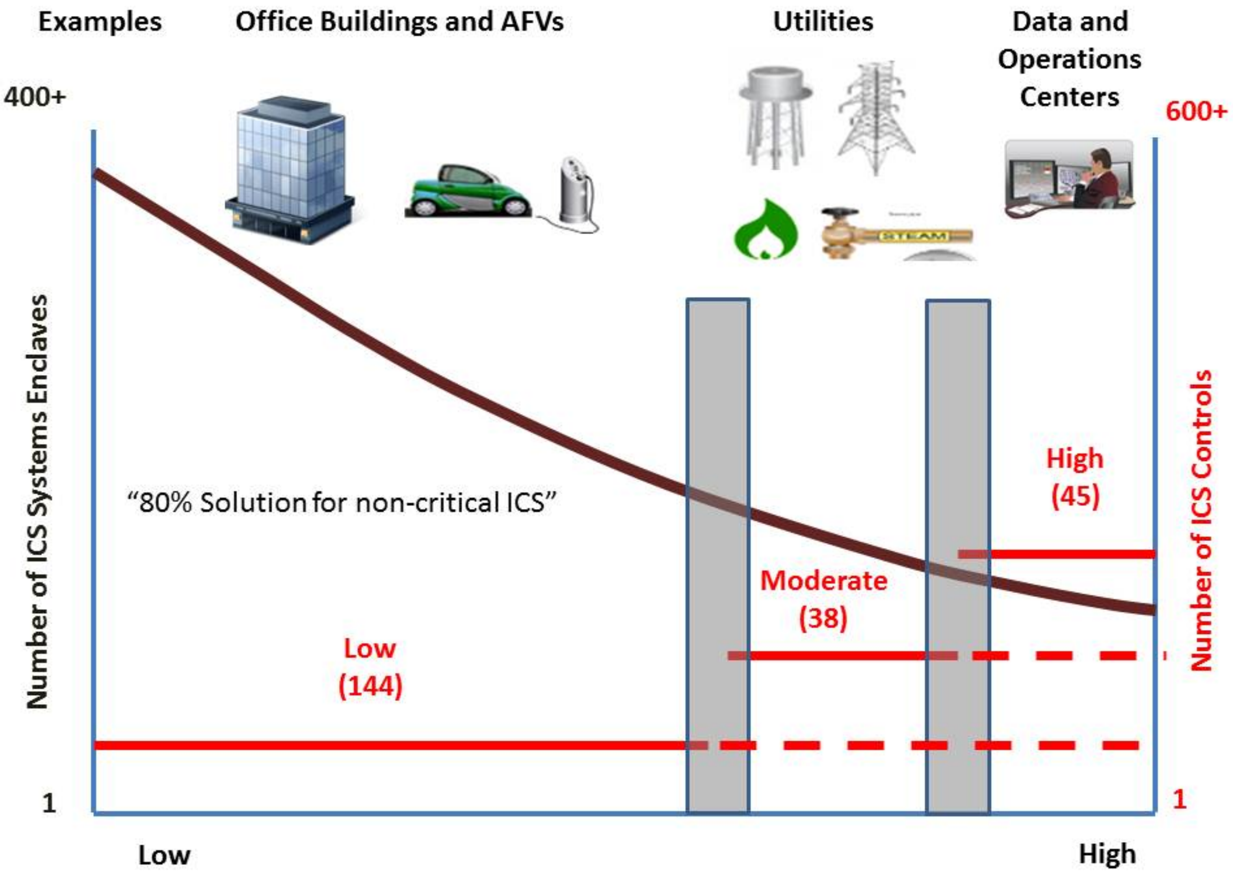


Figure 10 – ICSs Criticality

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 2011
- 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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	LOW	MODERATE	HIGH
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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	**LOW**	**MODERATE**	**HIGH**
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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	LOW	MODERATE	HIGH
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
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

INDUSTRIAL CONTROL SYSTEMS			
CONTROL	LOW	MODERATE	HIGH
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

<u>ICS Supplemental Guidance:</u> 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

<u>ICS Supplemental Guidance:</u> 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

<u>ICS Supplemental Guidance:</u> 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

<u>Control Enhancement:</u> (1)

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

PE-3 PHYSICAL ACCESS CONTROL

<u>ICS Supplemental Guidance:</u> 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.