Cybersecuring Industrial Control Systems

The Department of Defense is planning to adopt the NIST Risk Management Framework and will sunset the Defense Information and Accreditation Process.

BY MICHAEL CHIPLEY, PH.D., PMP, LEED AP, M.SAME, and DARYL HAEGLEY, OCP, CCO

Personnel of the 624th Operations Center, Joint Base San Antonio-Lackland, Texas, conduct cyber operations in support of the command and control of Air Force network operations and the joint requirements of Air Forces Cyber, the Air Force component of U.S. Cyber Command. U.S. AIR FORCE PHOTO BY WILLIAM BELCHER

The Department of Defense (DOD) is one of the largest owners of real estate, buildings and Industrial Control Systems (ICSs) in the federal government. DOD has more than 500 installations, 300,000 buildings, 250,000 linear structures and an estimated 2.5 million unique ICSs. These 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 are frequently real-time software applications or devices with embedded software.

This collection of specialized systems is pervasive throughout DOD's infrastructure. They are required to meet numerous, and often conflicting, safety, performance, security, reliability and operational requirements. ICSs range from non-critical Building Automation Systems (BAS) and Energy Management Control Systems to critical networks, such as the electrical power grid, Emergency Management Information Systems and Electronic Security Systems.

Within the controls systems industry, ICSs are often referred to as Operational Technology (OT) systems. Historically, the majority of OT systems were proprietary, analog and vendor supported, and were not internet protocol (IP) enabled. Systems key components, however—such as Remote Terminal Units, Programmable Logic Controllers, Physical Access Control Systems, Intrusion Detection Systems, closed circuit television, fire alarm systems, and utility meters—are now becoming digital and IP enabled. OT systems use Human Machine Interfaces to monitor the processes, whereas Information Technology (IT) systems use Graphical User Interfaces. Most current ICSs and sub-systems are now a combination of OT and IT.

As these systems and components became digital and IP enabled, interconnects to the organization network and business systems began to expose the organization to significant vulnerabilities. There was not a clear line of demarcation where one system started and one ended. For example, an Energy Monitoring and Control System meter could be on the utility SCADA system or on the building's BAS.

As is typical with other ICSs owner/ operators, DOD's systems have become potential cyber targets. New tools like Shodan that expose IP devices on the Internet, and malware such as Stuxnet, Flame, Duqu and Shamoon

are designed to steal technical information. They can simply create havoc or, worse, physically destroy critical infrastructure and key resources. There are a number of government efforts that are underway to review and ensure the cybersecurity of DOD ICSs.

ADAPTING WITH TECHNOLOGY

Advanced and emerging technologies such as the smart grid, smart buildings, smart meters and smart cars require internet connectivity. DOD has decided to adopt the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and sunset the traditional Defense Information and Accreditation Process (DIACAP). As an initial part of this process, the current DOD Information Assurance directive is being replaced with DOD Instruction 8500.01, "Cybersecurity" (currently in final coordination), which in turn adopts NIST SP 800-53 RMF. The target date for the instruction to be implemented is October 2013.

Within DOD, ICSs are defined as Platform IT (PIT), and must be evaluated for cybersecurity certification and accreditation. Working with the DOD Chief Information Officer staff and the Committee on National Security Systems (CNSS), the installations and environment community proposed an expanded the various DOD ICSs. Notably, the draft version of DOD Instruction 8500.01 "Cybersecurity," provides examples of "platforms" that may include PIT:

"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 systems, 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)."

COMPARING IT AND OT SYSTEMS

	Information Technology	Operational Technology
Purpose	Process transactions, provide information, computes solutions	Control or monitor physical processes and equipment
Architecture	Enterprise wide infrastructure and applications (generic)	Event-driven, real-time, embedded and interconnected hardware and software (customized)
Interfaces	GUI, Web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
Ownership	Chief Information Officer (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

In addition, the document requires each system to be formally designated.

"All DoD Information System and PIT systems will be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253 and will implement a corresponding set of security controls that are published in NIST SP 800-53 regardless of whether they are National Security System (NSS) or non-NSS."

In April 2012, I&E and CIO representatives formed a technical working group and undertook the task of creating the first CNSSI 1253 ICS-PIT Overlay:

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

REVIEW AND IMPLEMENTATION

After extensive collaboration among 65 government representatives spanning DOD, the Department of Homeland Security (DHS), General Services Administration and numerous other agencies, the working group delivered the first ICS-PIT Overlay to CNSS in January 2013. The Overlay is both a "primer," with a standard architecture and layers diagram, and a pictorial of typical devices, sensors and actuators that enable staff in the field to identify and understand the operational protocols, network ports and connections.

The draft version also was shared with the NIST SP 800-82 Joint Working Group and DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Cybersecurity Protection Program for inclusion into the Cybersecurity Evaluation Tool (CSET) version 5.1 to be used as an information and training document.

The initial ICS-PIT Overlay was DOD-centric and used DOD-specific parameters, but was formally adopted by CNSS in March 2013. However, recognizing the value of the ICS-PIT Overlay, CNSS requested the Overlay be generalized and made applicable to all CNSS stakeholders. The Overlay then was generalized and submitted to the CNSS in July 2013, with an expected approval and release date of October 2013.

Publication of the CNSSI 1253 ICS Overlay should occur about the same time as the final DODI 8500 Cybersecurity Instruction, with the intent that both finalized guidance documents will be integrated into the next version of the DHS CSET (version 6.0), which is scheduled for a November 2013 release.

FUTURE OUTLOOK

Once all relevant guidance has been published, the next steps to ensure the cybersecurity of DOD ICSs include developing specific policy guidance; beginning an inventory of DOD ICS systems; and implementing an automated anomaly detection, patch and vulnerability management capability.

It also will be necessary to implement workforce training for I&E and IA professionals. The program should integrate vulnerability and penetration testing as well as determine the skills and qualifications for Authorizing Officials to understand the relevant risks and unique configuration and operational characteristics of ICSs.

Michael Chipley, Ph.D., PMP, LEED AP, M.SAME, is a Consultant to the Department of Defense Installations and Environment Business Enterprise Integration Office; 571-232-3890, or mchipley@pmcgroup.biz This email address is being protected from spambots. You need JavaScript enabled to view it.

Daryl Haegley, OCP, CCO, is Program Manager, Department of Defense Installations and Environment Business Enterprise Integration Office; 571-232-2754, or daryl.haegley@osd.mil This email address is being protected from spambots. You need JavaScript enabled to view it. .