3-10-2010

Codifying Information Assurance Controls for Department of Defense (DoD) Supervisory Control and Data Acquisition (SCADA) Systems (U)

Eddie A. Mendezllovet

CODIFYING INFORMATION ASSURANCE CONTROLS FOR DEPARTMENT OF DEFENSE (DOD) SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

THESIS

Eddie A. Mendezllovet, Captain, USAF

AFIT/GCO/ENG/10-13

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GCO/ENG/10-13

CODIFYING INFORMATION ASSURANCE CONTROLS FOR DEPARTMENT OF DEFENSE (DOD) SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science

Eddie A. Mendezllovet, BS

Capt, USAF

March 2010

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GCO/ENG/10-13

CODIFYING INFORMATION ASSURANCE CONTROLS FOR DEPARTMENT OF DEFENSE (DOD) SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

Eddie A. Mendezllovet, BS

Capt, USAF

Approved:

//////SIGNED////// 15/03/2010

Lt Col Jeffrey W. Humphries, PhD (Chairman) Date

//////SIGNED////// 15/03/2010

Mr. Juan Lopez Jr. (Member) Date

//////SIGNED////// 15/03/2010

Dr. Kenneth M. Hopkinson (Member) Date

AFIT/GCO/ENG/10-13

Abstract

Protecting DoD critical infrastructure resources and Supervisory Control and Data Acquisition (SCADA) systems from cyber attacks is becoming an increasingly challenging task. DoD Information Assurance controls provide a sound framework to achieve an appropriate level of confidentiality, integrity, and availability. However, these controls have not been updated since 2003 and currently do not adequately address the security of DoD SCADA systems. This research sampled U.S. Air Force Civil Engineering subject matter experts representing eight Major Commands that manage and operate SCADA systems. They ranked 30 IA controls in three categories, and evaluated eight SCADA specific IA controls for inclusion into the DoD IA control framework. Spearman's Rho ranking results (ρ = .972414) indicate a high preference for encryption, and system and information integrity as key IA Controls to mitigate cyber risk. Equally interesting was the strong agreement among raters on ranking certification and accreditation dead last as an effective IA control. The respondents strongly favored including four new IA controls of the eight considered.

To my Wife, Children & Family

Acknowledgments

I would like to thank my advisor and committee members Lt Col Humphries, Mr. Juan Lopez Jr. and Dr. Hopkinson. Without their patience and their valuable time, this thesis would have never been possible. I would also like to thank my wife and children for their inspiration, motivation and encouragement. Lastly, I owe a great deal of gratitude to my parents for without them I certainly would not be the person that I am today; their continued sacrifices to provide their children with the chances and opportunities for a much better future.

Eddie A. Mendezllovet

Table of Contents

Page

List of Figures

List of Tables

CODIFYING INFORMATION ASSURANCE CONTROLS FOR DEPARTMENT OF DEFENSE (DOD) SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

I. Introduction

The evolution of critical infrastructure has experienced an unusually rapid maturity in the last decade due to the high influence of information technology and the Internet. Twenty years ago, "infrastructure" was defined primarily with respect to the adequacy of the nation's public works (Moteff and Parfomak, 2004). Recent threat developments have culminated in a series of laws, and executive orders to define infrastructure sectors and the corresponding assets considered being to be the most "critical". Vulnerability of these systems to cyber interruptions (intentional or unintentional) or exploitation due to internet connectivity has raised the level of information systems importance to critical infrastructure.

Information systems can add value to Industrial Control System (ICS) environments. Consequently, the number of information systems used in ICS has increased rapidly in recent years (Guttromson & Schur, 2007). ICSs are of critical importance to our nation as many are used to support a significant number of the national critical infrastructure. Besides adding value, the convergence of information systems and ICSs also threaten our nation by putting at risk our national critical infrastructure. (Throughout this thesis, Industrial Control Systems will be referred to as Supervisory Control and Data Acquisition (SCADA) systems for consistency and clarity).

Information security specialists have to artfully balance security versus operation. It is part of their job to allow enough flexibility for successful operations while protecting the systems and the data therein. Security professionals agree that SCADA systems are generally more complicated because of the convergence of increasingly dissimilar technologies in SCADA systems and business networks. As long as corporations continue to connect SCADA systems with business enterprise networks, the potential risks for cyber attacks will continue to increase (Ning, 2008).

This research focused on the current Department of Defense (DoD) Information Assurance (IA) controls published in 2003 and the current NIST ICS Security controls published in 2008. This thesis seeks to correlate the current set of IA controls framework to determine IA security control gaps specific to SCADA systems.

Problem Statement

Protecting our critical infrastructures from attack is a very difficult task. The government not only considers a vast number of infrastructure critical, but the fact that up to 85% of our critical infrastructure is owned by the private sector makes the problem even more challenging (Martin, 2006). Understanding the importance of ICSs, associated cyber risk, and how they are protected via IA controls is considered highly relevant for this effort. The adoption of information technology systems in an ICS environment and their convergence continue to increase our nation’s exposure to real and potentially catastrophic threats (GAO, 2004).

This research seeks to reduce the gap between security IA controls issued by DoD in 2003 and the current NIST ICS security controls published in 2008. Much has changed since 2003. There are currently a vast number of organizations engaged in various research efforts focused on SCADA and ICS security. The most recent DoD IA controls published in 2003 do not incorporate the new ICS IA controls published by NIST in 2008. This thesis attempts to generate ICS security controls corresponding to NIST publications and update the DoD IA controls, thus, producing a standard that can be applied to AF ICS.

Research Goals

The overall AFIT AF A4/7 research effort is to develop efficient methodologies for assessing AF critical infrastructures. For this phase of the effort, this thesis will review and correlate current National Institute of Standards and Technology (NIST) and Department of Defense (DoD) security controls, identify possible DoD Industrial Control Systems (ICS) security gaps, recommend new or modified DoD IA controls to close these gaps and validate security controls with subject matter experts from the AF civil engineering community. Finally, this thesis will assess what security controls the DoD ICS community believes are the most important.

Scope

This research is limited to mostly non-technical assessments of current government and Department of Defense (DoD) published standards, policy or regulation and the opinion of different subject matter experts from the AF civil engineering community.

Thesis Organization

The goal of this section is to provide a background for this research, establish its goals and scope and introduce the organization of this thesis. In order to discover Industrial Control Systems (ICS) security gaps in DoD Information Assurance (IA) security controls, one must understand the importance of ICS and information assurance. Chapter two provides the background of Industrial Controls Systems (ICS) and their importance to critical infrastructure. Next, SCADA and Information Systems (IS) network convergence, cyber connectivity trends, and critical infrastructure cyber exposures are discussed. The next section discusses the basics of protecting Information IS in the federal government and the DoD via IA disciplines. Chapter two concludes by bringing together IA security controls from the National Institute of Standard and Technology (NIST) and the DoD specific to SCADA systems. Chapter three present the methodology used in the study data collection procedures, and survey instrument, and the data analysis procedures. Chapter four presents the results of the data analysis. Chapter five discusses the conclusions and recommendations for future research.

II. Literature Review

Overview

This section covers, in very general terms, topics such as Industrial Control Systems (called SCADA throughout this document), Critical Infrastructure Protection, Information Assurance, Information Assurance Controls and the role different levels of our government play in attempting to protect their information assets. Equally important to the discussion is the importance of SCADA systems as they have become integral parts of our critical infrastructure and how different government agencies attempt to preserve their confidentiality, integrity and availability through the use of information assurance programs and IA controls. This section provides a high-level view of the government's SCADA IA effort and ends with a brief view of DoD specific efforts.

The U.S. has seen a significant and steady increase in cyber attacks on both traditional information technology (IT) networks and Critical Infrastructure Systems. Some of these information systems are at the core of our national critical infrastructure; hence greater efforts and attention are being directed towards securing these systems and cyber security has become a priority to our nation (Langevin & McCaul, 2008).

Not only is the government taking notice, but the mainstream media is now covering cyber security in much more detail. In the article "*America's Growing Risk: Cyber Attack. How enemy hackers threaten our nuke plants, pipelines and more,*" (Derene, 2009) discusses the possibilities of the enemy creating mass disruptions of services to SCADA by changing a few lines of computer code (Derene, 2009). These scenarios become more plausible as more organizations continue to integrate SCADA and business networks leading to an increased risk of cyber attacks.

Critical Infrastructure

The definition of critical infrastructure is constantly evolving (Lewis, 2006). The Marsh Report (1997) and Executive Order 13010 (EO-13010, 1998) provided an early definition of infrastructure:

"a network of independent, mostly privately-owned, man-made systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential foods and service" (Lewis, 2006).

The most current definition can be found in Homeland Security Presidential Directive 7, issued by President Bush in 2003:

"Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being" (Moteff &Parfomak, 2004).

Table 1. Critical infrastructure sectors (Brown et al., 2006)

Critical infrastructure sectors	
Information Technology	Public health, healthcare and food
Telecommunications	Drinking water and water treatment
Chemical	Energy
Transportation Systems	Banking and finance
Emergency Services	National monuments and icons
Postal and Shipping services	Defense industrial base
Agriculture	

Critical infrastructure is divided into 14 sectors, the sectors are provided in Table 1. These infrastructures have grown complex and interconnected, meaning that a disruption in one may lead to disruptions in others (Mosfett, 2008). Over the years, operators of these infrastructures have taken measures to guard against, and to quickly respond to, many of the intentional and unintentional threats (Mosfett, 2008). However, the protection of these sectors requires government agencies and the private sector to work in concert to try to find the best solutions for protecting our critical infrastructures. To best coordinate efforts and resources, Homeland Security Presidential Directive-7 selected eight agencies for each of the sectors. Table 2 provides a list of lead agencies and their corresponding responsibility for critical infrastructure.

Table 2. Critical Infrastructure Lead Agencies (Moteff &Parfomak, 2004)

Lead Agency	Critical Infrastructure
Dept. of Homeland Security	Information technology Telecommunications Chemical Transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems Emergency services Postal and shipping services
Dept. of Agriculture	Agriculture, food (meat, poultry, egg products)
Dept. of Health and Human Services	Public health, healthcare, and food (other than meat, poultry, egg products)
Environmental Protection Agency	Drinking water and waste water treatment systems
Dept. of Energy	Energy, including the production refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)
Dept. of the Treasury	Banking and finance
Dept. of the Interior	National monuments and icons
Dept. of Defense	Defense industrial base

Industrial Control Systems support a great number of our critical national infrastructures such as power generation, gas and oil pipelines, water and waste, etc. The number of information systems in critical infrastructures has increased rapidly in recent years (Guttromson & Schur, 2007). Information systems expansion and adoption by critical infrastructure operators can threaten our nation by putting our national critical infrastructure at risk.

Industrial Control Systems (ICS)

In this thesis, the terms Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Critical Infrastructure are generally used interchangeably to refer to the same systems. This thesis uses SCADA as a general term encompassing several types of controls systems including ICS, distribute control systems (DCS), and critical infrastructure systems.

SCADA systems are considered a specialized information system. However, unlike a “regular” information system, SCADA systems have been primarily designed with safety, availability, and reliability in mind. SCADA systems are a type of computer automation system that uses a central computer system, wide area communications technologies and a large number of Remote Terminal Units (RTUs), to monitor and control geographically distributed processes such as pipelines, electric power transmission, and waste water (Shaw, 2006).

Because SCADA systems are based on computer technology, their designs have evolved in step with advances in computer technology which means that as computer technology has developed, the designers of SCADA systems have incorporated these advances into these systems (Shaw, 2006). In addition, SCADA systems can be viewed as a system of systems where individual components contribute to the overall availability, integrity, and confidentiality of the entire system. The loss of a single component can bring down the entire system. This philosophy is embraced by the popular saying: “A system is only as strong as its weakest link.”

A SCADA system is basically used to fetch and present current data values to human operators typically located at a control center (Shaw, 2006). The control centers are usually located in a separate physical part of the factory and typically have advanced computation and communication facilities. Modern control centers have data servers, human-machine interface (HMI) stations, data historians, engineering workstations, and other servers to aid the operators in the overall management of the SCADA system (see

Figure 1). Control centers provides situational awareness of the systems and operations, dispatch repair crews when needed, and serve as the focal point during emergencies (Igure, 2008).

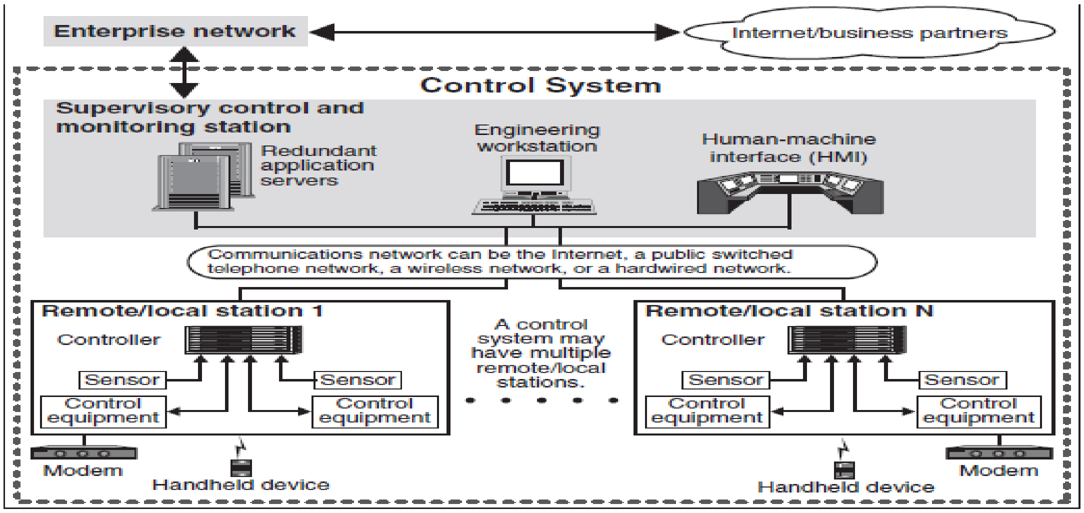

Enterprise network
Internet/business partners
Control System
Supervisory control and monitoring station
Redundant application servers
Engineering workstation
Human-machine interface (HMI)
Communications network can be the Internet, a public switched telephone network, a wireless network, or a hardwired network.
Remote/local station 1
Controller
Sensor
Sensor
Control equipment
Control equipment
A control system may have multiple remote/local stations.
Remote/local station N
Controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device
Handheld device
Modem

Figure 1. Typical Components of Industrial Control Systems (GAO, 2004)

SCADA networks are usually connected to the outside corporate network and/or the internet through specialized gateways (Igure, 2008). A SCADA network provides various connections for field devices or remote field sites via telephone, radio frequency (RF), satellite or wide area networks (see Figure 2.). These field devices, such as sensors and actuators, are monitored and controlled over the SCADA network at the control center. Communications on a SCADA network include control messages exchanged between master and slave devices. A master device is one which can control the operation of another device (i.e. PC, PLC). A slave device is usually a simple sensor or actuator which can send messages to the command device and carry out actions at the command of a master device (Igure, 2008).

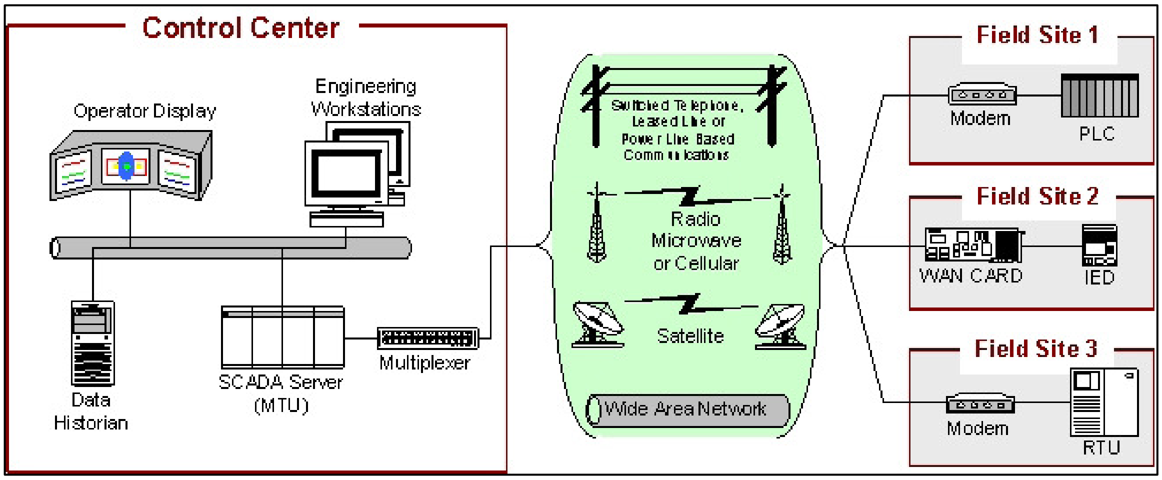


Figure 2. SCADA Control Center (Stouffer, 2005)

Many of these systems perform critical functions. In the electric industry for example, many of these systems perform critical bulk electric systems functions such as telemetry, monitoring and control, power plant control and real-time inter-utility data exchange. The loss or compromise of these systems would adversely impact the reliable operation of electric system assets, affecting part of our nation's critical infrastructure (Shaw, 2006).

Critical Infrastructure Protection (CIP)

There has been a variety of working groups, special reports, federal policies, and organizations addressing CIP issues (see Appendix A for evolution of CIP) (GAO, 2004). In recent years, the security community has grown more concerned about the physical and cyber vulnerability of critical infrastructures (Moteff, 2008). We know with certainty that in order to protect our national critical infrastructure against possible attacks, security specialists have to properly guard against physical and cyber threats alike.

The government's goal for CIP is to ensure that any disruptions of the services provided by critical infrastructures are infrequent, of minimal duration, and manageable (Moteff, 2008). CIP tries to counter and mitigate existing critical infrastructures threats. The official definition of CIP as defined in Presidential Directive 7 is: "the strategies, policies and preparedness needed to protect, prevent, and when necessary, respond to attacks on critical sectors and key assets" (Lewis, 2006).

Because about 85 percent of the nation's critical infrastructure is owned by the private sector, it is vital that the public and private sectors work together to protect these assets. To this effect, the Department of Homeland Security (DHS) is responsible for coordinating a national protection strategy including formation of government and private sector councils as a collaborating tool. The councils are to identify their most critical assets, assess the risks they face, and identify protective measures in sector-specific plans that comply with DHS's National Infrastructure Protection Plan (NIPP) (GAO, 2006).

In a press release (Nov 2009), Secretary Napolitano reaffirmed the government commitment to protecting our critical infrastructures:

"Securing our nation's critical infrastructure is vital to maintaining the safety of communities across the country; DHS is committed to working with federal, state, local, territorial and tribal partners, the private sector and the public to protect against threats to these assets—from cyber networks to drinking water."

Many of these critical infrastructure sectors have developed their own security practices and procedures. Many of these practices and procedures are applicable across industry boundaries to include the federal government. NIST has been working with a vast number of organizations to collect and codify this information to develop security control standards that can be tailored and applied across sectors. This unified security framework is crucial to protect our critical infrastructures, especially in the cyberspace domain.

Critical Infrastructure and Cyberspace

Globally-interconnected digital information and communications infrastructure underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security (Hathaway, 2009). Most modern industrial facilities (e.g. oil refineries, chemical factories, electrical power generation, and manufacturing) and associated critical infrastructures are largely dependent on these digital information and communications infrastructure.

The new Cyberspace Policy Review (2009) defines cyberspace as *"… the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."*

Operators rely heavily on cyberspace to monitor and control industrial systems. Because these networks are connected to the business network and the internet, operators are able to remote command and control these systems (Igure, 2008). This connectivity can help optimize manufacturing and distribution processes. It can also increase efficiency and reduce costs, but it also exposes the safety-critical industrial network to the myriad security problems of the internet (Igure, 2008).

Historically, security concerns were about protecting the physical nodes against physical attack, not protecting SCADA systems in cyberspace. This is no longer the case; it has become evident that critical infrastructures are also vulnerable to cyber attacks (Dancey, 2004). Several factors have contributed to the higher number of cyber threats to these systems: (1) the adoption of standardized technologies with known vulnerabilities, (2) the connectivity of control systems to other networks, (3) insecure remote connections, and (4) the widespread availability of technical information about control systems (Dancey, 2004).

Since 2001, 70% of reported incidents were due to attacks originating from outside the SCADA network (Igure, 2008). In a recent report published by the security company McAffe (2010), six hundred IT and security executives from critical infrastructure enterprises across seven sectors in 14 countries were surveyed. Topics of the survey included: their practices, attitudes and policies on security, the impact of regulation, their relationship with government, specific security measures employed on their networks, and the kinds of attacks they face (Baker et al., 2010). According to Baker et al (2010), the survey was not designed to be statistically valid. However, it provides a snapshot of views from a significant group of decision-makers. Additionally, the survey described in detail the way critical IT networks are defended and secured today.

Some of the more significant details provided in the report are:

- China reported the highest adoption rate of security measures
- Sectors with lowest adoption rate of security measures are water and sewage
- Sectors with highest adoption rate of security measures are energy and banking
- Foreign governments involvement in recent critical infrastructure attacks is high
- US and China are seen as “most potential” aggressors to critical infrastructure

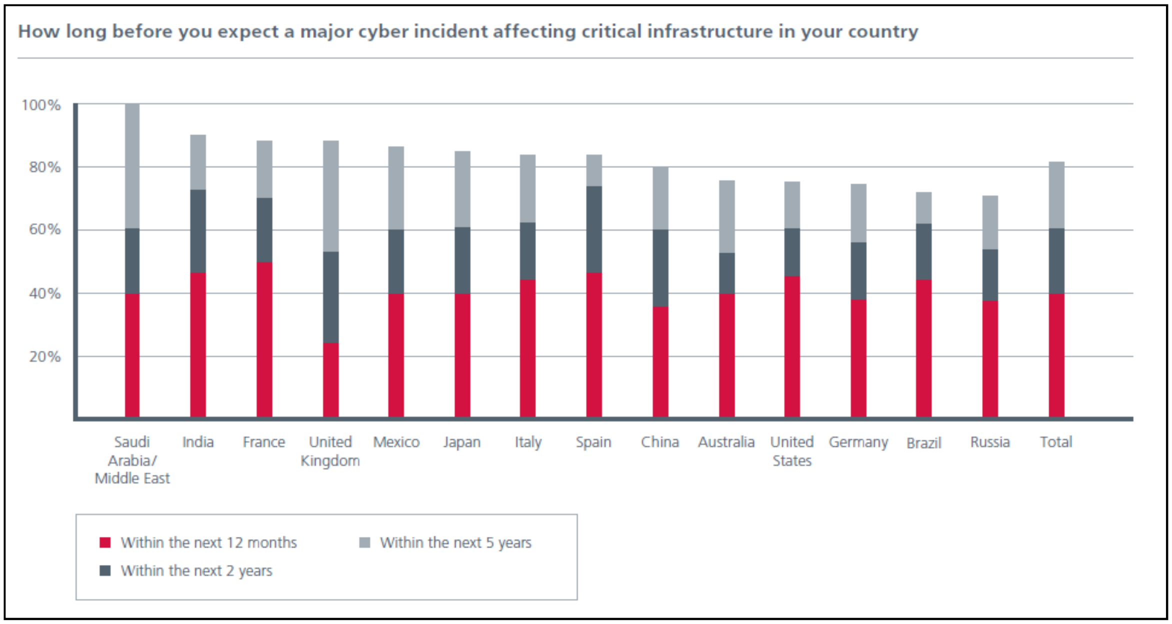


Figure 3. Time Base Expectancy of a Cyber Attack (Baker et al., 2010)

Countries expect critical infrastructure attacks in the near future. Figure 3 provides a bar graph illustrating which countries expect a critical infrastructure attack. These attacks are often leveraged by highly skilled operators and sponsored by foreign nations (Baker et al., 2010). The impact can vary depending on the severity of the attack and/or the facility targeted. Attacks can cost millions of dollars in lost revenues and damaged reputation. Survey participants also believe that attackers will become more skilled and resourceful (Baker et al., 2010).

The same sentiment was echoed by Mr. Dennis C. Blair, Director of National Intelligence during his 2010 annual threat assessment brief to Congress while speaking on the subject of cyber threats:

> "The national security of the United States, our economic prosperity, and the daily functioning of our government are dependent on a dynamic public and private information infrastructure, which includes telecommunications, computer networks and systems, and the information residing within. This critical infrastructure is severely threatened…The United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat awareness. Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication."

Information Assurance (IA)

What is information assurance? It is about protecting information from destruction, degradation, manipulation and exploitation (Blyth and Kovacich, 2006). Information assurance has many different meanings to many different people but a widely used definition for IA in the private sector is:

" IA defines and applies a collection of policies, standards, methodologies, services and mechanisms to maintain mission integrity with respect to people, process, technology, information and supporting infrastructure" (Willett, 2008).

Information has become a critical asset and a high value target for many competing interests. Therefore, information and information systems need to be protected and secured from unauthorized access, changes or disruptions. Information assurance provides a mean for an organization to protect their information and information systems.

As society increasingly relies on information systems, an effective IA program must be implemented that addresses technology, processes, and people. A failure of any one of these elements can adversely impact the availability, integrity, and confidentiality of systems and the information within. An effective IA program becomes more crucial as cyber attackers continue to improve their technical competencies, tactics, and techniques.

The DoD defines IA as:

> *"Actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities"*(DoDD 8500.1, 2002).

IA and the US Government

Technology advancements have improved many aspects of our lives but they have also given rise to various new problems (Senft and Gallegos, 2008). The government is coping with these new problems by trying to update laws, policy and regulations. Unfortunately, they generally lag behind new technological changes. Even when governments assume the role of defender, seeking to prevent attacks and improve security, many IT and security executives are skeptical about their ability to deter or protect against cyber attacks. Figure 4 compares the percentage of countries that believe their current laws are inadequate against cyber attackers.

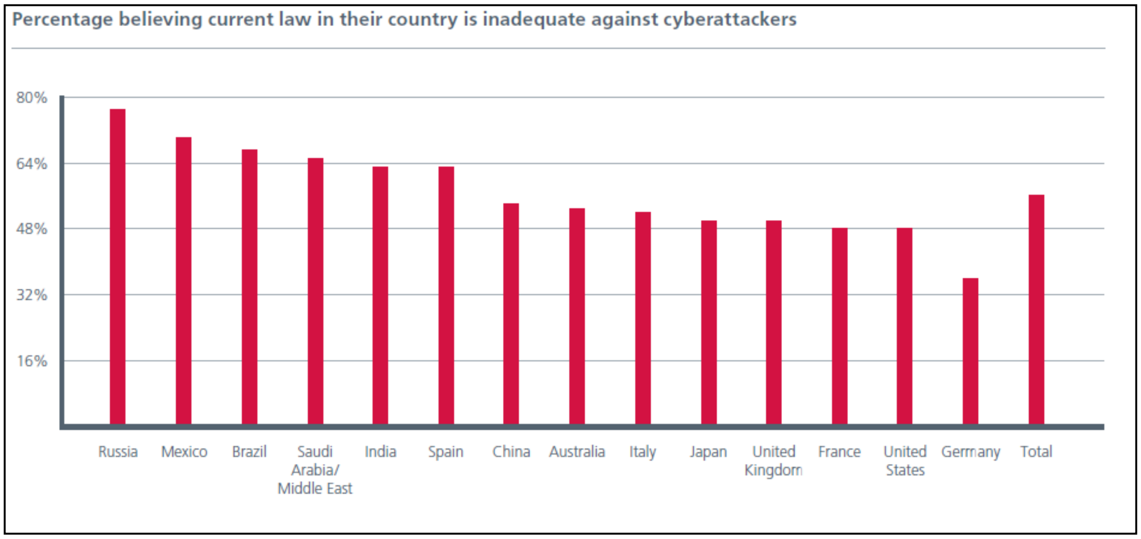


Figure 4. Laws Inadequate Against Cyber Attacks (Baker et al., 2010)

Reaction to serious events can be a great catalyst for quick government action. For example, major data breaches caused by hackers and stolen or lost laptops resulted in huge outcries by citizens prompting the government to enact new laws, policies and guidance (refer to Appendix C for a more comprehensive breakdown of some of these documents). For this research effort, the focus is directed toward documents related to the development of IA programs and security controls such as Appendix III to Office of Management and Budget Circular Number A-130 (OMB Circular No. A-130), and the Federal Information Security Management Act (FISMA).

OMB Circular No. A-130 in many ways engendered the need to establish and employ IA controls commensurate to information risk and affirmed the need to accredit and certify federal systems at least every three years (OMB, 2000). Appendix III re-orients the federal computer security program to better respond to a rapidly changing technological environment. It establishes government wide responsibilities for federal computer security and requires federal agencies to adopt a minimum set of management controls.

These management controls are directed at individual information technology users. Agencies are required to implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications (OMB, 2000). In addition, agencies need to review the security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system (OMB, 2000).

FISMA is the principal law governing the federal government's information security program. It requires federal government agencies to provide information security protections for agency information and information systems (Hulitt and Vaughn Jr, 2008). FISMA defined three security objectives for federal government information systems: (1) confidentiality, to preserve authorized restrictions on access and disclosure, with means for protecting personal privacy and proprietary information; (2) integrity, to guard against improper information modification or destruction while ensuring information non-repudiation and authenticity; and (3) availability, to ensure timely and reliable access and use of information. FISMA places significant requirements on federal agencies for the protection of information and information systems, and places significant requirements on the NIST to assist the federal agencies comply with FISMA (Ross et al., 2005).

FISMA required NIST to develop two mandatory Federal Information Processing Standards (FIPS) that apply to all federal information and information systems to include SCADA systems. However, these FIPS are not mandatory for the national security community and private sector. These standards are FIPS 199 and FIPS 200. FIPS 199 is a standard used for determining the security category of an information system. FIPS 200 is a standard stating the mandatory minimum security requirements that all federal information systems must meet (Katzke, Stouffer et al., 2006).

IA and the DoD

DoD policy mandates IA to be implemented in all systems and services acquisitions at levels appropriate to the system characteristics and requirements throughout the entire system life cycle (DoDI 8580.1, 2004). One of the key processes for implementing information assurance is the Certification and Accreditation (C&A) process.

DoDD 8500.1 requires that all DoD information systems be certified and accredited. Certification is defined as: "*The comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements*" (Lee et al., 2005).

Accreditation on the other hand is *"The formal declaration by the Designated Approving Authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk"* (Lee, S., G. Ahn, et al., 2005). The DAA is *"The official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk"* (Lee et al., 2005).

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) was one of the first processes to certify and accredit DoD systems. The DITSCAP Application Manual defines the DITSCAP as “the standard DoD process for identifying information security requirements, providing security solutions, and managing information systems security activities” (Lee et al., 2005). In 2006, the DITSCAP was superseded by the DoD Information Assurance Certification and Accreditation Process (DIACAP). DIACAP officially establishes DoD’s IA C&A process for authorizing the operation of DoD information systems. DIACAP is the DoD’s approach to implementing a C&A process that supports Net-Centricity (Tyler, 2006).

The DoD anticipates that almost everything will eventually interconnect making the standardization of protection levels for systems very important. This implies that there should be a standard for determining a protection level to enable uniformity across interconnections (Campbell, 2007). Table 2 provides a variety of C & A guiding documents for federal organizations.

Table 3. C& A Guiding Documents (Campbell, 2007)

Federal Entity	Guiding Document
DoD	DIACAP, DoDD 8500.1, DoDI 8500.2 & DoDI 8510.01
Intelligence	DCID 6/3
Other Federal Agencies	OMB A-130, NIST SP 800-37, NIST SP 800-53, NIST SP 800-60

The DIACAP implements and validates standardized IA controls across DoD information systems consistent with DoD regulatory policy (i.e. IA 8500 series) and legislative policy (i.e. FISMA) (Bendel, 2006). In addition, DIACAP is based on two principles: (1) IA is established via IA controls, and (2) IA controls need to be maintained.

The concepts of DoD IA controls were introduced in 2002 by DoDD 8500.1 and DoDI 8500.2. An IA control describes what the relevant safeguards and activities should provide (Campbell, 2007). All DoD information systems have to maintain an appropriate level of confidentiality, integrity, authentication, availability, and non-repudiation.

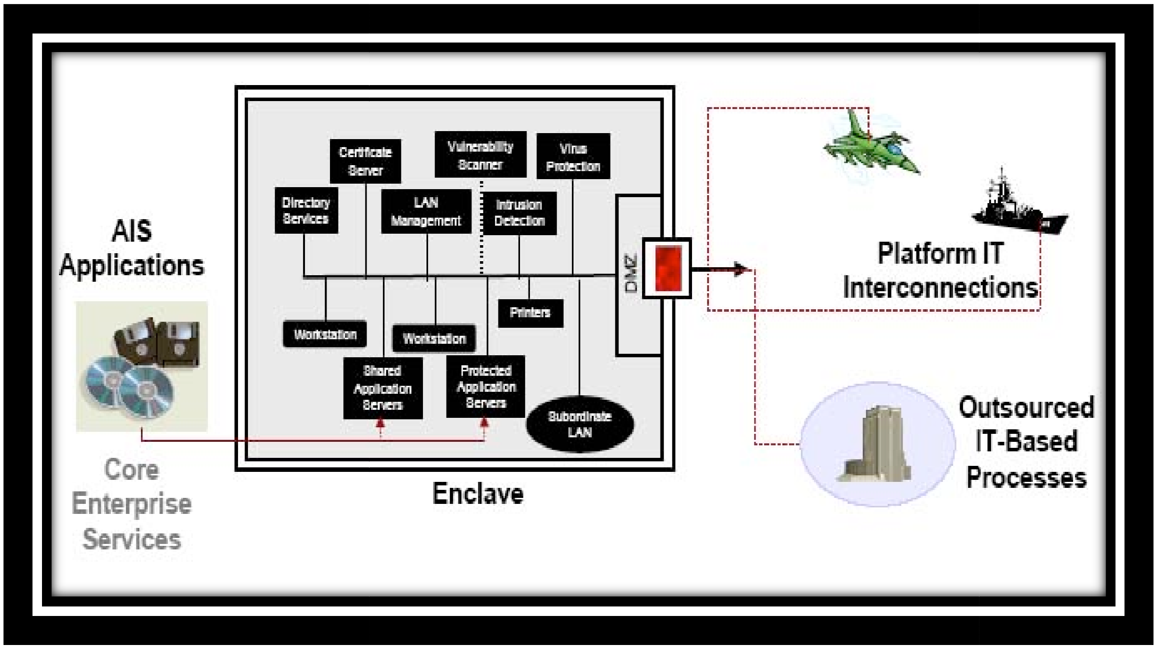


Figure 5. IS IA Categories (from Auburn.edu)

Due to the sheer number of systems and to make the program more manageable for IA professionals, DoD information systems are organized into the four categories: Automated Information System (AIS) applications, enclaves, outsourced IT-based processes, and platform IT (DoDI 8500.2, 2003). Figure 5 offers a logical representation of the four categories. Appendix D contains definitions for each of these categories.

Due to the "joint" nature of military operations and to continue to move towards DoD's net-centricity vision, the DoD has decided that a service C&A should be honored when connecting to a different service's network via a reciprocity agreement. DoD Memorandum (2009*), DoD Information System Certification and Accreditation Reciprocity*, "*mandates the mutual agreement among participating enterprises to accept each other's security assessment in order to reuse IS resources and /or accept each other's assessed security posture in order to share information."*

IA and ICS

Many SCADA systems in use today entered the workforce years ago, when security measures were not anticipated; system reliability and safety were primarily the focus. Securing SCADA systems simply meant: physically secure access to the network and the devices that controlled these systems (Katzke et al., 2006). The introduction of new information technologies makes it possible to connect vastly different networks -- to include the once isolated SCADA networks. SCADA networks are now able to connect to traditional business networks over the same information infrastructure.

A common misconception regarding SCADA networks is that they are isolated from outside networks (Igure, 2008). However, according to the McAffe report (2010), "*more than three quarters of those with responsibilities for ICS reported that they were connected to the Internet or some other IP network, and just under half of those connected admitted that this created an "unresolved security issue."* Business networks are perhaps better equipped to handle insecurities and have security tools designed to counter and mitigate threats, but many ICS components are unprepared to handle most common threats and malware (Wiles et al., 2008).

Neglecting or bypassing security measures can create a vast number of vulnerabilities Figure 6 illustrate the security measures adoption rates by country. Security vulnerabilities can also arise in a system because of problems in the system specification, the system implementation or during system operation (Igure, 2008). Attackers take advantage of these vulnerabilities to affect the integrity, availability, and confidentiality of these systems. Table 3 describes the most common general threats and effects of several of these attacks.

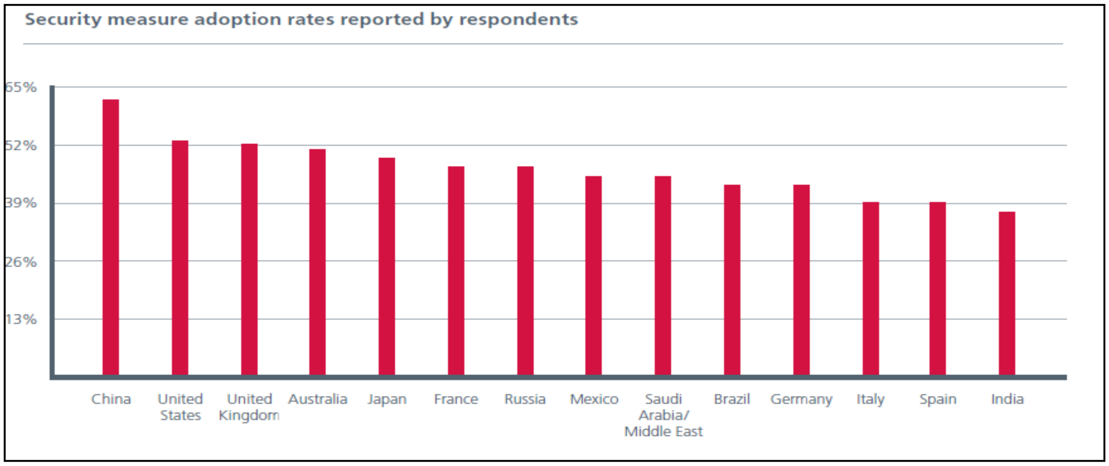


Figure 6. Security measures adoption rates (Baker et al., 2010)

The connectivity of SCADA networks with outside networks will continue to grow, leading to an increased risk of cyber attacks and a critical need to improve the security of SCADA networks (Igure, 2008). Many professional organizations are involved in the effort to improve SCADA network security (Igure, 2008). Many industry sectors have developed their own security standards, for example: the electric industry uses North American Electric Reliability Council (NERC) standards, the gas industry uses the American Gas Association (AGA) standards.

Table 4. General threats and attack effects (Igure, 2008)

General Threat	Effect of Attack
Modifying system/user data	Loss of data integrity; Secondary effects could be loss of availability
Alter/Destroy stored data	Loss of data
Modify message content Change control signals Change data points/set points Change operator display value	Loss of data/message integrity; Secondary effects could be loss of availability; Presenting wrong information to human operators could have adverse effects
Sniffing data/control messages	Loss of confidentiality
Block/reroute communications	Loss of availability
Shut down devices	Loss of availability
Plan malicious code	Could cause all kinds of disruptions depending on intent of attack

US Government and ICS IA

The major US government SCADA security objectives are: (1) restrict logical access to the SCADA network, (2) restrict physical access to the SCADA network and devices, (3) protect individual SCADA components from exploitation, (4) maintain functionality during adverse conditions, and (5) restoring systems after an incident (SP 800-82, 2008). The government believes that the most successful methods for securing a SCADA system is to gather industry recommended practices and engage in a proactive, collaborative effort between all stake holders (SP 800-53, 2009).

As previously mentioned, FISMA required NIST to develop two mandatory Federal Information Processing Standards (FIPS). To support both FIPS 199 and FIPS 200, NIST developed Special Publication (SP) 800-53, "*Recommended Security Controls for Federal Information Systems*." SP 800-53 requires federal agencies to implement one of three minimum (baseline) sets of security controls for all information system in the agency based on the systems' security categorization (2006).

It is important to point out that SP 800-53 was first developed to address traditional IT systems, not SCADA systems. In time, SP 800-53 has adopted security controls specific to ICS. NIST has worked cooperatively with the SCADA communities in the public and private sectors to develop specific guidance to apply the security controls SCADA systems. SCADA-specific guidance is included in NIST SP 800-53, Revision 3, Appendix I: Industrial Control Systems – Security Controls, Enhancements, and Supplemental Guidance (Stouffer et al., 2008).

If automated mechanisms are not readily available, cost-effective or technically feasible, then compensating security controls implemented through non-automated mechanisms or procedures should be employed (SP 800-53, 2009). Compensating controls are alternative safeguards and countermeasures that accomplish the intent of the original security controls that could not be effectively employed (SP 800-53, 2009).

In 2006, NIST released the *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security* (SP 800-82) to addresses vulnerabilities, threats, and security controls (Katzke et al., 2006). Section 6 of the document provides initial guidance on how 800-53 security controls apply to ICS's. See Appendix D for a list of ICS specific controls (Stouffer et al., 2008). Following the NIST guidelines is mandatory for federal agencies; however, it is voluntary for nongovernmental organizations and private agencies.

NIST SP 800-82 provides an overview of ICS's system topologies, identifies threats and vulnerabilities to an ICS, and provides recommended security countermeasures to mitigate the associated risks. Specific recommendations and guidance are provided in an outlined box for each section throughout the document. In addition, Appendix C provides an overview of the many activities currently ongoing among federal organizations, standards organizations, industry groups, and automation system vendors to make available "best practices" in the area of ICS security (Stouffer et al., 2008).

Organizations are encouraged to tailor the recommended guidelines and solutions to meet their specific security and business requirements (Stouffer et al., 2008). A single security solution is not adequate to properly protect ICS's. An effective cyber security strategy should apply a defense-in-depth approach. A combination of policy and security controls can be very effective. The publication provides three types of security controls: management, operational and technical (Stouffer et al., 2008).

NIST IA Controls

NIST security controls are derived from multiple communities (defense, financial, healthcare, and intelligence) and are applicable to any organization (SP800-53, 2009). The selection and implementation of appropriate security controls for information systems are important tasks that can have major implications on the operations and assets of an organization (SP800-53, 2009). To successfully implement security controls, organizations must (1) select a security control baseline, (2) tailor the baseline security controls, and (3) supplement the tailored baseline as necessary.

Table 4 provides a listing of the NIST SP 800-53 security controls. They are grouped into three classes (1) management, (2) operational, and (3) technical controls. Security controls should be employed in conjunction with and as part of a well-defined and documented information security program (SP800-53, 2009).

Table 5. SP 800-53 Security Control (SP800-53, 2009)

ID	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessments and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Management controls are controls that focus on the management of risk and the management of the organization systems (Stouffer, 2005). Operational controls are security controls primarily implemented and executed by personnel as opposed to the system (Stouffer, 2005). Technical controls are security controls primarily implemented and executed by the organization through mechanisms contained in the hardware, software or firmware components of the system (Stouffer, 2005).

To identify each security control, a numeric identifier is appended to the family identifier to indicate the number of the control within the family. For example, AU-5 is the fifth control in the Audit and Accountability family. The security control structure consists of the following components: (1) a *control* section, (2) a *supplemental guidance* section, (3) a *control enhancements* section, (4) a *references* section, and (v) a *priority* and *baseline allocation* section. The following is an example of a control from the Personnel Security family, control number 2 taken from SP 800-53, Appendix F:

PS-2 POSITION CATEGORY

Control: The organization:

a. Assigns a risk designation to all positions

b. Establishes screening criteria for individuals filling those positions

c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*]

Supplemental Guidance: Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria includes an explicit information security role and appointment requirements (e.g., training, security clearance).

Control Enhancements: None.

References: 5 CFR 731.106(a).

Priority and Baseline Allocation:

P1	**LOW** PS-2	**MOD** PS-2	**HIGH** PS-2

SECURITY CONTROL SECTIONS

Control section: The control section provides a concise statement of the specific security capabilities needed to protect a particular aspect the information system.

Supplemental section: The supplemental guidance provides important considerations for implementing security controls in the context of an organization's operational environment, mission requirements, or assessment of risk. Security control enhancements may also contain supplemental guidance.

Security control enhancements: The control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to the basic control functionality based on the results of a risk assessment.

References section: The references section includes a list of applicable federal laws, Executive Orders, directives, policies, standards, and guidelines that are relevant to a particular security control or control enhancement.

Priority and baseline allocation: The priority and baseline allocation section provides: (1) the recommended priority codes used for sequencing decisions during security control implementation, and (2) the initial allocation of security controls and control enhancements for low-impact, moderate-impact, and high-impact information systems.

DoD and ICS IA

The DoD relies on SCADA systems that control critical infrastructure processes maintained by both the defense sector and private industry to support its mission and operations. To help find IA solutions for SCADA systems, the Deputy Under Secretary of Defense for Science & Technology encouraged the Small Business Technology Transfer (STTR) program to sponsor research focused on information assurance of SCADA systems (OSD, 2009). For example, proposal OSD09-T003, is asking for the development of innovative software and data protection technology that improves the security of SCADA and Distributed Control Systems (DCS).

DoD working groups are coordinating efforts to transition DoDI 8500.2 IA controls to those contained in the NIST 800-53 (DIACAP, 2010). This indicates that the DoD ICS C&A guidance will be revised in the future. However, the DoD currently has no specific C&A guidance for SCADA systems. ICS are considered a subset of platform IT (PIT) systems. These systems physically interact with the environment and only perform information processing assigned to it by its hosting special purpose system (ETL 9-11, 2009). Normally, C&A is not required for PIT. However, security requirements must be addressed in system design and operation as prescribed in current guidance and policy. If the PIT has connectivity to an external network then the C&A process is required as a PIT Interconnection (PITI) (ETL 9-11, 2009).

The C&A process for PITI is mandatory regardless of the persistence of the boundary interconnection (e.g., always-connected Ethernet, wireless connection, dial-up connection). PITI refers to network access to PIT and has readily identifiable security considerations and needs that must be addressed in both acquisition and operations (ETL

9-11, 2009). IA controls listed in *Information Assurance (IA) Implementation* (DoDI 8500.2), and draft, *Guide to Industrial Control Systems Security* (NIST SP 800-82), are designed to complement each other when addressing the uniqueness of PIT or PITI (ETL 9-11, 2009).

DoD IA Controls

IA controls establish baseline levels of availability, integrity and confidentiality of any given system depending on the mission assurance category (MAC) and confidentiality needs. Due to limited resources and vast competing interests, DoD information systems have to be categorized in importance or mission impact levels, particularly the combat mission. The MAC level reflects the importance of information relative to the achievement of DoD goals and objectives. The DoD has defined three MAC levels and are listed and defined in Table 5. MAC I requires the highest level of integrity and availability, whereas MAC III requires the lowest.

Table 6. Mission Assurance Categories (DoDI 8500.2)

Mission Assurance Category (MAC) Levels:	Data Mission Impact
I	Data is vital to the mission. The consequences of loss of integrity or availability of a MAC I system are unacceptable. Mission Assurance Category I systems require the most stringent protection measures (DoDI 8500.2 para E2.1.38.1).
II	Data is important to the mission. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance (DoDI 8500.2 para E2.1.38.2).
III	Data is necessary for the conduct of day-to-day business, but does not materially affect the mission. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices (DoDI 8500.2 para E2.1.38.3).

The baseline set of IA controls are pre-defined based on determination of the MAC and Confidentiality Levels (CL) as required by the information system owner. The baseline IA Controls for each of the combinations of MAC and CL are outlined in the enclosures to DoDI 8500.2 (AFI 33-200, 2008). Confidentiality levels are primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations, interconnection controls and approvals, and acceptable methods by which users may access the system (e.g., intranet, internet, wireless) (DoDI 8580.1, 2004). The DoD has defined three confidentiality levels. Table 6 list the definition of each confidentiality level.

Table 7 Confidentiality Levels (DoDI 8580.1, 2004)

Confidentiality Level	**Definition**
Classified	Systems process classified information
Sensitive	Systems process sensitive information to include any unclassified information not cleared for public release
Public	Systems process publicly releasable information

There are four parts to each IA Control:

1. Subject Area**:** One of eight groups indicating the major subject or focus area.
2. Control Number: Unique identifier comprised of four letters, a dash, and a number. The first two letters are an abbreviation of the subject area, the second two letters are an abbreviation of control name and the number represents a level of robustness.

3. Control Name: A brief phrase describing the individual IA control
4. Control Text: Description of IA condition or state that the IA control is intended to achieve.

Table 8. DoD IA Control Subject Areas (DoDD 8500.2)

Abbreviation	Subject Area Name	Number of Controls in Subject Area
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3
		Total = 157

Table 8 provides a listing of the DoDD IA subject areas and abbreviations. Figure 7 illustrates an example of the IA control taxonomy. Table 9 provides an example for data at rest of an IA control with varying levels of robustness. ECCR-1 calls for NIST certified cryptography while ECCR-3 calls for more stringent NSA-approved cryptography. The higher the control level number, the highest the level of robustness.

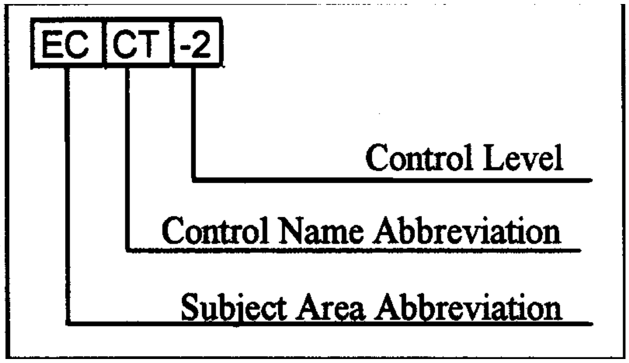


Figure 7. DoD IA Control Taxonomy (DoDD 8500.2)

The DAA or DoD community of interest representatives may add additional IA controls to locally augment the security baseline control set, only if the augmented controls will increase the security established by the enterprise baseline IA controls (DIACAP, 2010). There are security guides designed to help implement IA controls such as the Security Technical Implementation Guides (STIG).

Table 9. IA Control Example

IA Control	Control Level	MAC	Subject Area	Control Name	Definition
ECCR-1	1	II	Enclave Computing Environment	Encryption for Confidentiality (Data at Rest)	If required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.
ECCR-2	2	II	Enclave Computing Environment	Encryption for Confidentiality (Data at Rest)	If required by the information owner, NIST-certified cryptography is used to encrypt stored classified non-SAMI information.
ECCR-3	3	II	Enclave Computing Environment	Encryption for Confidentiality (Data at Rest)	If a classified enclave contains SAMI and is accessed by individuals lacking an appropriate clearance for SAMI, then NSA-approved cryptography is used to encrypt all SAMI stored within the enclave.

III. Methodology

Overview

This chapter presents the research methodology and statistical procedures used during this research effort. This chapter will present the survey instrument design, the data collection method, the sample selection criteria, and the statistical procedures used to analyze the data gathered.

Mapping DoD and NIST IA Controls

Comparing and mapping IA controls from the NIST SP 800-82 to the DoD IA Control framework is the primary focus of this research endeavor. A comprehensive list of ICS IA controls were carefully scrutinized for clarity in definition, applicability to DoD control systems, and persistent semantic translation. A numbered coding schema was constructed to map the linkages between IA control items. An example of the coding schema and associated definitions are provided in Table 10. The final coding schema and associated mappings are provided in Appendix F.

Table 10. Correlation Codes

Code	Definition
8	NIST requirement and DoD IA control are equivalent
9	NIST requirement is more specific than the DoD IA control
11	NIST requirement has no counterpart in the DoD IA control
17	NIST requirement is less specific than the DoD IA control

Comparing security controls produced by different organizations is difficult and subject to interpretation (Katzke et. al, 2006). While the mapping discussed in this thesis represents a significant effort by a number of experts, there are no guarantees that the mapping is completely accurate or correct (Katzke et. al, 2006). Controls were compared using semantic analysis to preserve the definition, intent and meaning of the IA control. IA controls that deviated from these areas were deferred to the survey instrument for subject matter experts resolution.

If substantial agreement can be achieved among the civil engineering SME community, then the recommended definition can be a potential IA control candidate. This procedure is consistent with other similar efforts and is considered adequate to make comparisons and draw some conclusions (Katzke et. al, 2006). Although the granularity and level of abstraction of the security control sets being compared are not always the same, using a SME consensus approach preserves precision of definition and minimizes differences in interpretation and judgment (Abrams, 2007).

Survey Instrument

The survey instrument is divided into three sections. Section one contains five questions related to demographic information of the participants, section two contains a listing of control area categories in a table format for ease of creating rankings, and section three contains eight recommended IA security controls for evaluation by participants using a 5-point Likert scale. The survey instrument design combines recommended best practices from a variety of sources to derive a specific set of IA controls that can be incorporated into the DoD IA control framework. Many ICS or SCADA IA controls map to the DoD framework with no translation required. However, other IA controls were so specific to ICS or SCADA that some interpretation or translation is required. The survey contains the set of ICS or SCADA IA controls that require:

(1) translation to fit into an “existing” DoD IA control subject category

or

(2) interpretation to fit into a "newly created" DoD IA control subject category

SME participants were asked to rank NIST ICS IA control categories in what they perceive is most important to day-to-day operations. Additionally, subjects were asked to rate the measurement of agreement on proposed modifications to existing DoD IA controls and the addition of new DoD IA controls. This survey should provide feedback about the security controls the DoD ICS community feels are most important to secure ICSs. Additionally, the survey should help gauge if those priorities are being met by the current DoD IA controls.

Pilot Survey

The survey instrument was pilot tested by with two groups of personnel. One group had little IA control exposure and focused on testing the functionality, layout, and the clarity of instruction of the survey instrument. The second group had varying degrees of exposure to IA controls and tested the items, definitions, and reasonableness of the survey instrument. The pilot survey personnel consisted of graduate students attending the Air Force Institute of Technology. Their feedback resulted in changes to various questions, rewording instructions, and changing various elements of the layout design to improve readability.

Population

The target population is USAF Industrial Control Systems subject matter experts (SMEs) from the civil engineering community. The sample was drawn from personnel stationed at various bases located with the Continental United States (CONUS) and Outside the Continental United States (OCONUS) representing as many major commands as possible. The personnel included in the sample were specifically targeted because they met the following criteria:

- They represent a good cross section of the USAF population of Civil Engineer subject matter experts
- They have been exposed to management principles for securing control systems from cyber threats through industry certification or other formally recognized education
- They have a vested interest in getting this right for the USAF and the DoD community
- They volunteered to participate in the study

Sampling Strategy

The sampling procedure used for this research was convenience sampling. A convenience sample is a procedure where the subjects are selected, in part or in whole, at the convenience of the researcher. This approach is a specific type of non-probability sampling which involves the sample being drawn from that part of the population which is readily available. In this case, the desired sample should consist of a good cross section of U.S. Air Force personnel from the civil engineering community. Furthermore, it is desired to achieve a good cross sectional representation of U.S. Air Force major commands.

Research Approval

The Air Force Institute of Technology (AFIT) Institutional Review Board (IRB) reviewed and approved the study and survey instrument for this research. Additionally, this study qualified for an IRB exemption because it contains research activities in which the only involvement of human subjects was covered by an exemption category. Appendix I contains the AFIT IRB waiver approval.

Additionally, in accordance with Air Force Instruction 36-2601, all surveys administered to U.S. Air Force personnel must first be approved and assigned a survey control number by the Air Force Survey Branch (AFSB) at the Air Force Personnel Center (AFPC). An acceptable alternative to AFSB approval is to obtain a commanders approval to conduct the survey of U.S. Air Force personnel. Permission to survey U.S. Air Force civil engineering personnel was authorized by the Air Force Civil Engineering Support Agency (AFCESA). Appendix G contains the AFCESA approval memorandum.

Data Collection Method

The survey instrument was electronically distributed to the respondents via electronic mail (email) as an attached document. All participants were asked to respond with a digitally signed email as a measure of validating the identity and authenticity of the respondent in an online environment. This procedure is feasible because the participants are expected to use a DoD Common Access Card (CAC) to access email services. As an additional measure to preserve anonymity, the participant email address was inserted into the blind carbon copy field. This technique is a reasonable measure to preserve the secrecy of the intended recipient in email communications. Responses were stored on a network server in a password protected folder at the Air Force Institute of Technology. The survey instrument is provided in appendix H.

Data Analysis Procedures

The data analysis phase of this study focused on (1) describing the perceived importance of NIST ICS security controls to the day-to-day operation of DoD ICS controls and (2) the level of agreement among SMEs to recommended new and modified DoD IA controls specific to ICS. Part one consists of matched pairs of rankings that measure the strength of the association and perceived importance of Security Control Area categories among US Air Force civil engineering SMEs. Part two, consists of eight recommended ICS security controls that address gaps in the current DoD IA controls framework. The next section will describe the procedures for both parts.

Part I: Paired Rankings

Respondents were randomly assigned into one of two groups. Ranked responses were rank ordered from 1 through k items for each group. Ties were resolved by preserving group bias towards the frequency of higher rank frequency count for each element. In rare case that an absolute tie occurs, the element will be averaged over the tied element. The Spearman rank correlation coefficient (rho) non-parametric statistical test is employed to measure association for the paired rankings (Conover, 1980). This statistic reflects the degree of association between the ranks of the responses. Association is a depiction of the relationship between two variables, but does not indicate any causal relationship (Gibbons, 1976).

Table 11. ICS IA Controls Grouped Rankings

Control Area Category (Rankings: 1 - 4)		Group 1	Group 2
Mgmnt Controls	Risk Assessment		
	Planning		
	System and Service Acquisition		
	Certification, Accreditation, and Security Assessments		
Control Area Category (Rankings: 1 - 15)		**Group 1**	**Group 2**
Operational Controls	Personnel Security		
	Physical & Environmental Protection		
	Control Center/Control Room		
	Portable Devices		
	Cabling		
	Contingency Planning		
	Disaster Recovery Planning		
	Configuration Management		
	System and Information Integrity		
	Malicious Code Detection		
	Intrusion Detection and Prevention		
	Patch Management		
	Media Protection		
	Incident Response		
	Awareness and Training		
Control Area Category (Rankings: 1 - 11)		**Group 1**	**Group 2**
Technical Controls	Identification and Authentication		
	Password Authentication		
	Physical Token Authentication		
	Role-Based Access Control		
	Web Servers		
	Virtual Local Area Network		
	Dial-up Modems		
	Wireless		
	Audit and Accountability		
	Encryption		
	Virtual Private Network (VPN)		

Typically the quality of ordered categorical data is determined from repeated measurements on the same subject in order to assess the level of agreement between raters, scales or occasions. Since repeated measurements are not incorporated into the research design, randomly assigning raters to a group for rank-ordered analysis helps to preserve the quality of ordered categorical recordings. Consequently, this procedure helps to identify large departures of inter-rater bias. Table 11 is an illustrated example of the group rank-ordered items used for the study.

Spearman's Rank Correlation Coefficient (Rho)

Rho is a non-parametric measure of the linear relationship between two variables. When using Spearman's rho, the null hypothesis indicates the absence of an association between the two tested variables. The alternative indicates the existence of an association between the variables. It is similar to the parametric version of Pearson's product-moment correlation coefficient except it is adjusted for ranked observations (Gibbons, 1976).

This study provided three sets of data for the participants to rank. Set one consists of 4 Management controls items, set two consists of 15 Operational controls, and set three consists of 11 Technical controls. The rankings are in perfect agreement if the ranks for each item are identical. They are in perfect disagreement if the ranks are in complete reverse order (Gibbons, 1976).

The differences between the ranks are used as a measure of their disagreement (Gibbons, 1976). This measure of disagreement (R) ranges from -1 to 1. When R = 0 there is no association and therefore no agreement or disagreement between the overall rank comparisons. Similarly, when R = -1 of R = 1, there is either perfect disagreement or perfect agreement, respectively, between the overall rank comparisons. The sign of the R statistic indicates the direction of association, not the strength of association (Conover, 1980). Figure 9 provides the formula for computing Spearman’s rank correlation coefficient (Conover, 1980):

$$\text{Spearman\_R} = 1 - \frac{6\left[\sum_{i=1}^{n} \left(\text{Group 1 - Group 2}\right)^{2}\right]}{n \cdot \left(n^{2} - 1\right)}$$

Figure 8. Spearman's Rho (Conover, 1980)

Part II: Recommended ICS Security Controls

Part two consists of 8 recommended ICS controls for comparison and interpretation of definitions. Measurement level is operationalized through a 5-point Likert scale. The scale range allows the respondent to choose varying degrees of agreement as follows: (1) strongly disagree, (2) disagree, (3) neutral, (4) agree and (5) strongly agree. All five responses are equally weighted. The 5-point Likert scale is a “higher better” metric meaning the higher, the value the more favorable the attitude and agreement with the recommendation provided for the participant. A description and analysis are presented in the next chapter.

IV. Data Analysis

The main goal of this research is to ascertain if there is more than marginal consensus among the US Air Force civil engineering SME community for recommended information assurance controls to address security concerns specific to DoD SCADA systems. This chapter presents an overview and analysis of the survey results using the statistical procedures previously discussed in the methodology section.

Demographic Information

Demographic information was collected from the participants during the survey process. This information was collected in order to help ensure that the sample was representative of the desired population as well as for future research. The demographic portion of the survey contained 5 questions.

Question 1: Major Command Representation

Participants were asked to list which major command (MAJCOM) they are associated with. Figure 12 provides the MAJCOM representation distribution of the respondents across the U.S. Air Force.   In total, 8 out of 10 (80%) of the MAJCOM's are represented in the sample. The two MAJCOM's not represented were the Air Force Global Strike Command (AFGSC) and U.S. Air Forces Europe (USAFE). Both of these organizations were targeted for sampling. However, no subjects from either organization volunteered to participate in the survey. One reason for the lack of participation from AFGSC could be that the command was recently created in December 2009 and is focused on their responsibilities for the U.S. nuclear arsenal.

One reason for the lack of participation from USAFE could be the subjects perceive their controls systems hosted in foreign countries are potentially outside the scope of this research effort. Future research in this area should ensure that these two MAJCOM's are adequately represented. USAFE units are primarily located throughout Europe and utilize sufficiently different equipment vendors and SCADA protocols. Therefore, the results of this research should be validated with USAFE to ensure applicability to their SCADA environment.

Question 2: Experience

Participant experience with the management or operation of SCADA systems was collected. The participants were asked to select their experience level from a list of the following five time periods:

- less than 1 year
- 1 – 3 years
- 4 -7 years
- 8 – 11 years
- 12 or more years

Table 11 illustrates the distribution of experience among the respondents. The results indicate that 70% of the respondents have 7 or less years of experience with the remaining 30% having extensive experience (i.e. 12 or more years). One interesting note is that 20 percent of the respondents have between one and three year and 20 percent have less than one year. This finding is interesting in that 40 percent of the participants are somewhat new to ICS. Although the data does not allow for a rigorous statistical analysis, the data indicates that 70% of the sample exhibit moderate experience levels. It is not known why the sample did not contain experience levels at the 8 – 11 years.

However, this gap is not expected to bias the results since the next higher tier is represented in the sample.

Table 12. Respondent experience in years

Years of Experience	Percent of Subjects
Less than one year	20%
1 to 3 years	20%
4 -7 years	30%
8 to 11 years	00.0%
12 or more	30%

Question 3: Cyber Security Education

Participants were asked to list any computer or network security training they have completed during their career. The training covered a wide range of subject areas and was evenly spread across the group. The cyber security orientation of the sample is considered advanced based on the content of the topic areas provided by the respondents. Although there are a significant number of respondents relatively new to ICS, the sample appears to have a diverse background in cyber security education and training. Figure 10 provides the cyber security training distribution of the sample.

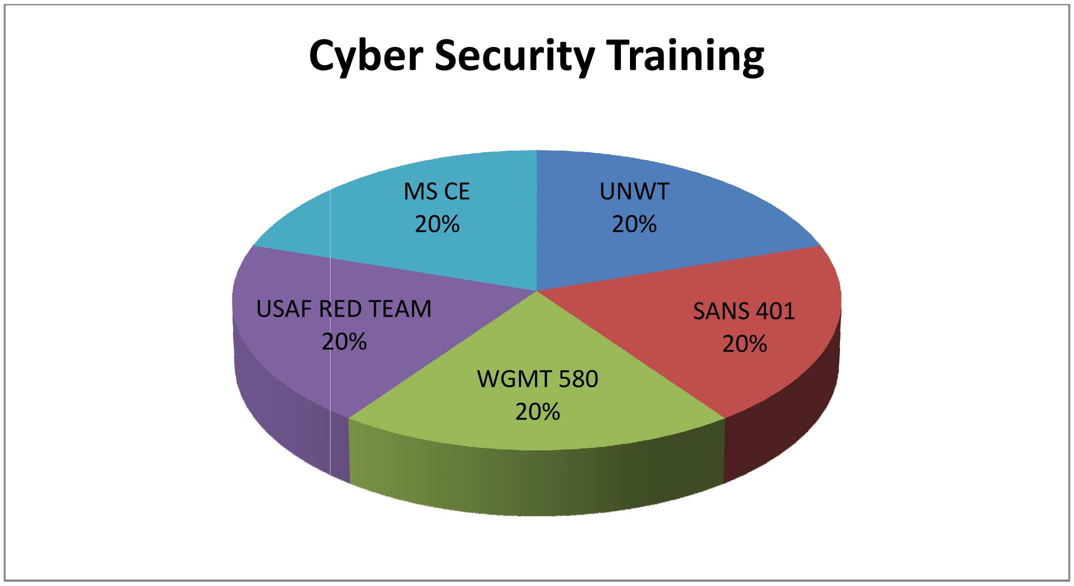


Figure 9. Sample Cyber Security Training

Question 4: Cyber Security Certifications

In addition to education and training, respondents were asked to list any security or IT certifications they hold. Certifications demonstrate knowledge in specific subject areas and ranged from server/client operations to network/infrastructure security. Some of the listed certifications are vendor specific such as Cisco Certified Network Associate (CCNA) and Server Plus (Server+). Other certifications listed are intended to be vendor neutral such as the Certified Information Systems Security Professional (CISSP) and Security Plus (Security+). Certifications are intended to validate a baseline level of knowledge or skill level. DoD has similarly adopted this philosophy and has implemented certifications as an essential component of professionalizing the IA workforce.

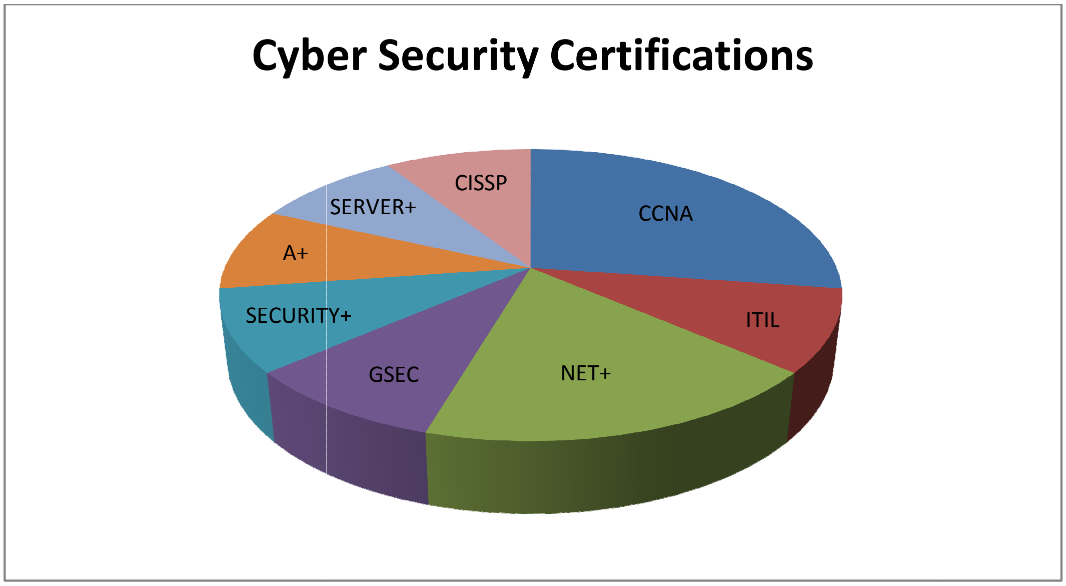
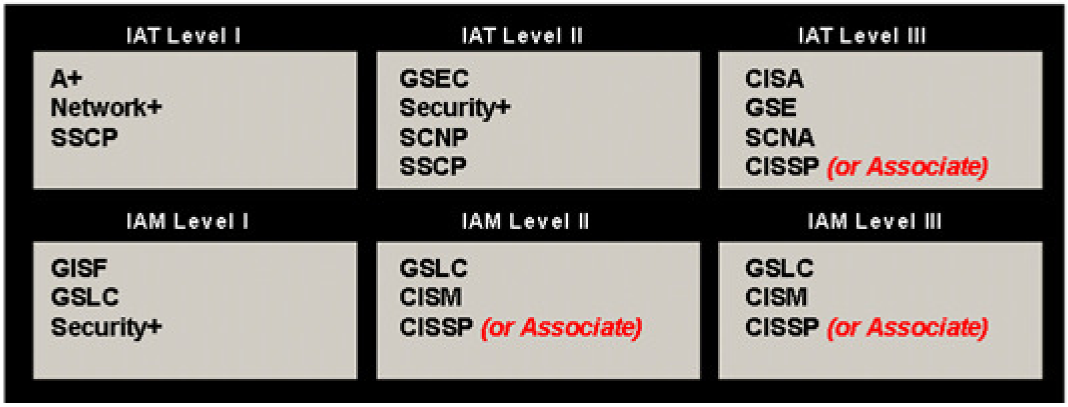


Figure 10. Sample Cyber Security Certifications

In total, 8 specific certifications were represented in the sample profile (Figure 11). 5 out of the 8 certifications are contained within the DoD IA certification rubric outlined in the DoD IA Workforce Improvement Program. Figure 12 provides the DoD Directive 8570 rubric segmented by technical and managerial categories and expertise levels. DoD personnel configuring, managing, and executing privileged access of SCADA systems are included in the IA workforce. The distribution of cyber security certifications among the sample provide sufficient evidence that the USAF CE community is well represented as part of the professional IA workforce. Furthermore, this indicates that the SME feedback will most likely be grounded on sound security principles underlying the framework for IA controls.



IAT Level I	IAT Level II	IAT Level III
A+ Network+ SSCP	GSEC Security+ SCNP SSCP	CISA GSE SCNA CISSP *(or Associate)*
IAM Level I	**IAM Level II**	**IAM Level III**
GISF GSLC Security+	GSLC CISM CISSP *(or Associate)*	GSLC CISM CISSP *(or Associate)*

Figure 11. DoD Approved Baseline Certification (DoDD 8570)

Question 5: Government Affiliation

The final question in the demographics section asked the respondents to identify the affiliation with the government. The possible selections were (1) contractor, (2) military (Reserve, Guard, or Active Duty), (3) Civil Service employee, or (4) other. If the respondent selected "other", they were asked to provide a description. In addition, the respondents were asked to select all categories that apply. This would allow the respondents to select multiple categories to ensure that appropriate coverage was considered. For example, there are civil service employees that are also serving in the US Air Force Reserve as a civil engineer. In this scenario, the participant could identify their affiliation as a civil service employee and a US Air Force Reserve employee.

Table 13 provides the government affiliation distribution. The sample contains no contractors, 40% military (75% active duty, 25% reserve, and 0% guard), and 60% civilians. This mixture provides an adequate representation of the CE community across the US Air Force enterprise. This study achieved an adequate balance in the affiliation representation.

Table 13. Government Affiliation Distribution

Government Affiliation	Percent of Subjects
Contractors	0 %
Civil Service	60%
Military	40%
-Active Duty (75%)	
-Reserve (25 %)	

IA Controls Rankings

The next section of the survey instrument asked the participants to rank the various security controls. Security controls are fundamental safeguards or countermeasures prescribed for an informational system to protect the confidentiality, integrity, and availability of the system and its information (Stouffer, K., J. Falco, et al., 2008). The security controls are grouped according to functional activities required to implement a safeguard or countermeasure and are identified as a (1) management control, (2) operational control, or (3) technical control. Participants were asked to independently rank the controls within each category in order of importance to the management or day-to-day operation of SCADA systems. This approach will help to capture and identify the perceptions of CE community personnel toward IA controls.

Since repeated measurements for each respondent will not be conducted during this research, the respondents were randomly assigned to one of two groups. Random assignment of respondents to one of two groups for rank-ordered analysis helps to preserve the quality of ordered categorical recordings. Consequently, this procedure helps to identify large departures of inter-rater bias. Furthermore, creating two groups prepares the data for statistical analysis using the Spearman’s rank correlation procedure.

The sample size is $n = 10$. The random assignment process placed respondents 1, 3, 5, 8, and 10 in group A, and respondents 2, 4, 6, 7, and 9 in group B. The ranked responses for each group in each security control category were tallied and rank ordered from 1 through k items. Table 14 provides the group ranked data elements to compute Spearman's rho statistic figure 9. The rho statistic for this data set is $\rho = .972414$.

To determine if this result is statistically significant, the ρ must be compared to a table of critical values for Spearman's Rho. The level of significance for this research is set at $\alpha = .05$. Table 15 shows that the critical value for $n = 30$ (grouped pairs) at $\alpha = .05$ is .364. Since $\rho = .972414 > .364$ we can conclude that the obtained result is statistically significant at the .05 level of significance. This result is substantial and provides sufficient evidence to conclude that any high level of agreement or disagreement among the respondents is not likely to occur by chance.

At this juncture, closer scrutiny of the rankings among the respondents by control group category will be analyzed. Rankings among the CE SME community will provide insight of their perceptions of the importance of IA controls relevant to SCADA systems. This information will be used in conjunction with part III of the survey instrument to provide depth to the interpretive analysis of the 8 recommended IA controls.

Table 14. Group ranked data and Spearman's Rho computation

	Group A Ranking	Group B Ranking	D	D^2
Mgmt Controls	1	1	1	1
	3	2	-1	1
	2	3	0	0
	4	4	2	4
Operational Controls	5	3	0	0
	2	2	-3	9
	10	13	-3	9
	12	15	0	0
	14	14	-2	4
	9	11	0	0
	6	6	-3	9
	7	10	0	0
	1	1	-2	4
	3	5	0	0
	4	4	3	9
	11	8	3	9
	15	12	6	36
	13	7	-1	1
	8	9	0	0
Technical Controls	1	1	0	0
	3	3	-3	9
	7	10	-2	4
	2	4	0	0
	8	8	1	1
	10	9	0	0
	11	11	-1	1
	6	7	0	0
	5	5	2	4
	4	2	3	9
	9	6	0	0
			sum	124
			rho	***0.972414***

Table 15. Critical values for Spearman's Rho (Zar, 1982)

	α level of significance		
N	**0.05**	**0.02**	**0.01**
5	1	1	N/A
6	0.886	0.943	1
7	0.786	0.893	0.929
8	0.738	0.833	0.881
9	0.683	0.783	0.833
10	0.648	0.746	0.794
12	0.591	0.712	0.777
14	0.544	0.645	0.715
16	0.506	0.601	0.665
18	0.475	0.564	0.625
20	0.450	0.534	0.591
22	0.428	0.508	0.562
24	0.409	0.485	0.537
26	0.392	0.465	0.515
28	0.377	0.448	0.496
30	0.364	0.432	0.478

Ranked Management Controls

All respondents had strong agreement with the 1 - 4 rankings of management controls. They had perfect agreement for item 1 (Risk Assessment) and item 4 (Certification, Accreditation & Security Assessments (C&A)). Item 2 (System and Service Acquisition) and item 3 (Planning interchanged positions between the two groups which clearly places these two items in the middle of the rankings. There is no surprise that risk assessment was ranked number one by the CE SME community. Risks associated with safety, health, environment-related or economic typically result in unrecoverable consequences (Stouffer, et al., 2008).

Item 4 – Certification, Accreditation and Security Assessment

What was most revealing among the four rankings in management controls is the placement of Certification & Accreditation last. C&A is a process that ensures that systems and major applications adhere to formal and established security requirements that are well documented and authorized. C&A is required by the Federal Information Security Management Act (FISMA) of 2002. All systems and applications that reside on U.S. government networks must go through a formal C&A before being put into production, and every three years thereafter. Since accreditation is the ultimate output of a C&A initiative, and a system or application cannot be accredited unless it meets specific security guidelines, clearly the goal of C&A is to force federal agencies to put into production systems and applications that are secure. This is counter to the perception expressed by the CE SME community.

Considering that management controls only address a mere 4 items in the management control category (as compared to 15 operational controls and 11 technical controls), one would expect C&A to rank high on the list since the process places emphasis on the system meeting specific security requirements. Further research should be conducted in this area to ascertain what the contributing factors for this perception gap are. Table 16 lists the final combined group rankings for the management controls category.

Table 16. Ranked Management Controls

Rank	Management Controls
1	Risk Assessment
2	System and Service Acquisition
3	Planning
4	Certification, Accreditation, and Security Assessments

Ranked Operational Controls

In the operational control category, the top five ranked controls in order of importance are (1) System & Information Integrity, (2) Physical and Environmental

Protection, (3) Personnel Security, (4) Malicious Code Detection, and (5) Intrusion Detection and Prevention. There was no serious disagreement among the CE SME community with the top five operational controls. Some rearrangement between items 3 (Personnel Security) and 5 (Intrusion Detection and Prevention) occurred but not substantial in position to warrant disparity among raters. The bottom three ranked controls were (13) Media Protection, (14) Portable Devices, and (15) Cabling. These bottom three rankings did not reveal substantial disagreement in rankings and is not surprising. Interesting findings for operational controls were in perfect agreement in item 1 (System and Information Integrity), and moderate disagreement between items 6 (Disaster Recovery) and 10 (Contingency Planning).

Item 1 – System and Information Integrity

Information and System Integrity as the number one ranked item under operational controls is a substantial finding. Table 17 provides the final ranked operational controls.

Table 17. Ranked Operational Controls

Rank	Operational Controls
1	System and Information Integrity
2	Physical & Environmental Protection
3	Personnel Security
4	Malicious Code Detection
5	Intrusion Detection and Prevention
6	Disaster Recovery Planning
7	Configuration Management
8	Awareness and Training
9	Patch Management
10	Contingency Planning
11	Incident Response
12	Control Center/Control Room
13	Media Protection
14	Portable Devices
15	Cabling

Traditionally, SCADA systems were designed as standalone networks with little to no connectivity to outside networks or systems. They are designed to be monitored through Human Machine Interface (HMI) on a 24 hour-7 days a week basis with little system interruption. Under these operating conditions, SCADA systems did not exhibit significant vulnerabilities to system and information integrity issues. However, the rapid increase in the use of internetworking protocols and connectivity to enterprise networks now make SCADA systems increasingly vulnerable to system and information integrity issues. The CE SME community is likely to have developed an aptitude for recognizing this vulnerability based on the exposure to the type of cyber security education and cyber security certifications they have received (see Figure 10 and 11). The importance of this observation when considering the 14 other operational controls the respondents could choose from cannot be overstated. This is an operational control priority among the CE SME community.

Item 6 & 10 – Disaster Recovery and Contingency Planning

Although both groups had perfect agreement of the ranking for disaster recovery (ranked number six), there was moderate disagreement of the ranking for contingency planning ranked number (Group A ranked 7, group B ranked 10). Although the definitions are closely related and have considerable overlap in application, there persists disagreement on their importance in the rankings. This might be related to the (1) distributed nature of SCADA systems across a large geographic region, and (2) the continued upward trend to utilize Internet Protocols for communications paths. Geographic spread and their associated physical boundary for contingency planning can be rationalized and is rather trivial to visualize. However, logical boundaries and the continued blurring of where SCADA network ends and the Enterprise network begins along with the associated responsibilities for contingency planning become more difficult to plan for.

Ranked Technical Controls

In the technical control category, the top five ranked controls in order of importance are (1) Identification and Authentication, (2) Encryption, (3) Role Base Access Control, (4) Password Authentication, and (5) Audit & Accountability. There was no serious disagreement among the CE SME community with the top 5 technical controls. Some rearrangement for between items 2 (Encryption) and 4 (Password Authentication) occurred but a not substantial in position to warrant disagreement among raters. Table 18 provides the final ranked technical controls.

Table 18. Ranked Technical Controls

Rank	Technical Controls
1	Identification and Authentication
2	Encryption
3	Role-Based Access Control
4	Password Authentication
5	Audit and Accountability
6	Virtual Private Network (VPN)
7	Wireless
8	Web Servers
9	Physical Token Authentication
10	Virtual Local Area Network
11	Dial-up Modems

What is interesting in this segment is how high they ranked encryption. Encryption is typically the method by which to operationalize confidentiality as a security goal. Confidentially is usually ranked very low as a security goal in a SCADA environment.

The confidentiality, integrity, availability (CIA) triad is a widely used information assurance model that identifies three fundamental security characteristics (Harris, 2003) Confidentiality provides some degree of assurance for data privacy. It is a well known system engineering principal that encryption can degrade the operational performance of the system (Stouffer, K., J. Falco, et al., 2008). It is also known that availability is a major design goal for SCADA systems. Therefore, it is an interesting finding that the CE SME community would rank encryption number two for technical controls.

Analysis of this finding is a bit difficult to interpret. However, one possible explanation is the perception and alignment gap between confidentiality and integrity among the respondents. SCADA system traffic does not typically contain messages that require privacy assurance of content unlike traditional information systems that store, process, display, and transmit email messages or corporate documents. A possible explanation is the misconception of the CE SME community of the security goal that is provided by encryption. They potentially desire to ensure the integrity of response messages during data acquisition and command messages during supervisory control. This position is reinforced by the fact that the (1) respondents placed significant value in System and Information Integrity under the operational controls (ranked number one) coupled with the (2) moderate amount of cyber security education and cyber security certifications of the respondents. Encryption can be deployed as part of a comprehensive security plan. However, encryption is not an appropriate mechanism, in most cases, to ensure integrity on SCADA networks. Additional research should be conducted in this area to further explain the alignment gap between confidentially and integrity among the CE SME community managing and operating SCADA systems.

IA Controls Agreement Measurements

The final section of the survey instrument contained 8 recommended IA controls for the participants to review. Of the 8 questions provided, the first three questions recommend IA control definitions that are not adequately addressed in the DoD IA controls framework but could fit under an existing IA control category. Five additional questions recommend IA control definitions and additionally recommend a new sub-category to be added to the DoD IA controls framework. Semantic translation of the NIST definitions preserved the intent of the specific IA control and made it adaptable to the DoD IA control framework.

The definitions and associated IA Control category and subcategory were provided in a table format for ease of comparison by each evaluator. The participants were asked to express their level of agreement, using a 5-point Likert scale, with the following criteria; (1) appropriate fit under the major DoD IA control category, (2) conciseness of the definition, and (3) appropriateness of the new sub-category. Table 19 provides a summary of the responses for all respondents.

Table 19. DoD IA Controls Response Summary

Part A: Incorporating ICS security control wording to existing DoD IA controls					
	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Q1: Role Based Access Control to ECLP	00%	00%	10%	50%	40%
Q2: Dial-up Modem to EBRP	00%	10%	00%	40%	50%
Q3: Web Servers to EBRP	00%	30%	10%	20%	40%
Part B: New DoD IA controls encompassing ICS security not covered by DoD					
	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Q4: Physical Environment Toxic substance (PETS)	00%	00%	10%	50%	40%
Q5: Physical Environment Blast Protection (PEBP)	00%	10%	20%	20%	50%
Q6: Physical Environment Access Controls to ICS Devices (PEAD)	00%	30%	10%	40%	20%
Q7: Physical Environment Transmission Medium Protection (PETP)	10%	00%	00%	30%	60%
Q8: Security Design and Configuration Virtual Partitioning (DCVP)	00%	00%	10%	50%	40%

IA Controls Response Summary Analysis

In order to conduct an analysis of the responses collected, the data was bifurcated into two major categories. Responses that were affirmative (agree and strongly agree) were placed in the Agree group. Responses that were negative (disagree and strongly disagree) were placed in the Disagree group. Responses with a neutral response were excluded from the analysis. Figure 13 contains the results of the two group comparison listed by question. The following sections will provide a narrative discussion and analysis of the results collected.

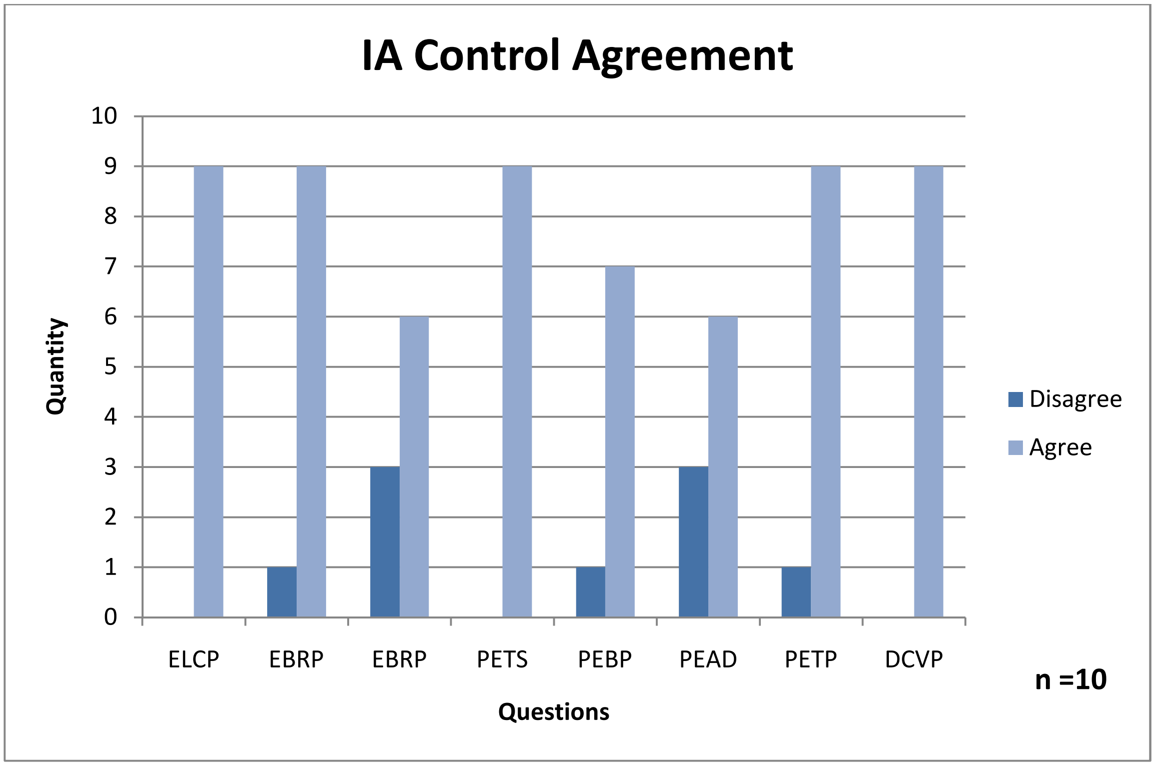


Figure 12. IA Control Agreement

Part A: Questions 1 - 3

Question 1: There is strong SME consensus to add Role Based Access Control (RBAC) into the Least Privilege DoD IA control subcategory. This result is not surprising since the SME's ranked RBAC number 3 of 11 in the technical controls category.

Question 2: There was slight disagreement from the respondents for placing dial-up modems under the Remote Access Privilege Function DoD IA control subcategory. The disagreement is primarily due to a difference in philosophy on remote access among the respondents. Some subjects stated that as long as the proper security measures were implemented, allowing remote dialing would be appropriate. Currently, USAF

Engineering Technical Letter 9-11 mandates the implementation of a voice protection system (VPS) which has a dial back feature. To illustrate the disagreement, in vivo extracts collected from respondents are provided below.

One respondent believes this is an adequate security safeguard to restrict remote access by dial-up modem and states, "[…] *it has the ability to do logging activity with other policy enforcement. The Voice Protection System would add another layer of protection for all Dial-up Modems in an ICS*."

Another respondent disagreed and stated that "[…] *no remote access should be permitted; only voice-capable modems should be allowed for after hours alarm notifications."* The final disagreement was essentially over the definition specificity. It was suggested that the DoD IA controls, as currently written, properly cover general practices and do not require additional details to describe form and function. Given the extensive use of modems in SCADA systems, this item remains open for additional discussion and clarification from the SCADA community at large.

Question 3: There was no consensus on the issue of Web servers as a product option in SCADA system. The respondents were evenly split on this topic. Web Servers are now offered as product options on historian servers for access outside of control rooms. Furthermore, Programmable Logic Controllers, and other control devices are increasingly being offered with embedded web and email servers to generate email notifications when certain conditions occur. This is an entirely new area for SCADA systems and operators alike. Traditional use of these services causes confusion for SCADA personnel when these services are made available on a control system. This partially explains the split decision from the CE SME community. A better understanding of how Web services can or should be incorporated into control systems is largely unexplored and causes this item to remain an open issue. Additional discussion and clarification from the SCADA community at large is required to resolve this item.

The disagreement is primarily due to subjects not seeing the addition of web, ftp, and email capabilities fitting into the Remote Access for Privilege functions category. Subjects see it fitting better under a least privileged type of category or a totally new category. Also, subjects stated that there is no reason for remote access outside of the control room. There may some rare cases for remote access due to ICS isolation from the base. Just like Q2, the final disagreement was about wording. The DoD IA covers general practices and does not go into details pertaining equipment, there is no need to make it more explicit or detailed for types of functions.

Part B: Questions 4 - 8

Question 4 & 5: There is also majority consensus for including questions 4 (Environmental Control Systems – HVAC) and question 5 (Control Center/Control Room) as new subcategories in DoD IA controls. However, both questions contained neutral responses (1 and 2 respectively) and were omitted in the agree/disagree determination.

Question 6: There is moderate disagreement in the definition and category placement of question 6 (Portable Devices). Respondents provided narrative that indicates that there is considerable variation in defining portable devices in a SCADA environment. The main issue is in an expanded version of portable includes portable equipment used by field engineers that fall outside the traditional definition of portable devices in the IT arena. Further work in this area is needed to more succinctly define the scope and function of portable devices as they specifically apply to the SCADA environment. This item will remain open for further discussion by the SCADA community at large.

Question 7: There is strong SME consensus to add question 7 (Cabling) as a new subcategory (Transmission Medium Protection) under the Physical and Environment DoD IA control category. The respondents ranked this control last (15 of 15) in the technical controls category. This does not make it any less important and must be addressed in any formal cyber risk assessment of a SCADA environment.

Question 8: There is strong SME consensus to add question 8 (Virtual Local Area Network - VLAN) as a new subcategory (Virtual Partitioning) under the Security Design and Configuration DoD IA control category. This is not a surprising result. VLAN architecture is rapidly advancing as a technique to partition portions of the SCADA from an enterprise network. Although the technique is gaining momentum among the IT community that must provide service to SCADA components inside the enterprise network (e.g. historian server or HMI) the security benefits are not well understood at this juncture. This item should be considered for inclusion in the DoD IA control framework with an expanded definition.

V. Conclusions and Recommendations

Conclusions

There is moderate consensus among the US Air Force civil engineering SME community for recommended information assurance controls to address security concerns specific to DoD SCADA Systems. Some DoD IA control definitions should be modified (listed in chapter IV) to include explicit language relevant to SCADA systems.

The research methodology applied in this study appears to be a sound approach to conduct an initial estimate of gaps in the current DoD IA control framework. The study resulted in providing insight into the perceptions of the U.S. Air Force civil engineering SME community concerning 30 IA controls across three categories. Ranking results (ρ = .972414) indicate a high preference for encryption, and system and information integrity as key IA Controls to mitigate cyber risk. Equally interesting was the perfect agreement among raters on ranking certification and accreditation last as an effective IA control. Additionally, the respondents strongly favored including four new IA controls of the eight they considered. Several issues remain open and should be explored with a larger SME community to reach a consensus.

Recommendations for Future Research

Questions that remain unresolved in this study should be fielded to a wider SME community and perhaps expanded to other service components. For example, SMEs indicated a high preference for encryption as a key IA control to mitigate cyber risk while ranking certification and accreditation last as an effective IA control. This is highly concerning as the DoD IA community relies very heavily on the C & A process to ensure systems confidentiality, integrity and availability. It is reasonable to infer that the DoD SCADA community finds that the C & A process is lacking or is inadequate to protect SCADA. Further research should be conducted on this area.

The AF Civil Engineering Support Agency created Engineering Technical Letter (ETL) 09-11: *Civil Engineering Industrial Control System Information Assurance Compliance* to provide technical guidance and criteria for information assurance of civil engineering ICS's. Future efforts can be directed at field-testing ETL 9-11 implementation requirements. A thorough analysis of first and second-order effects caused by ETL 9-11 implementation requirements can be helpful in accurately forecasting future needs resulting from ETL 9-11. For example, proper ETL implementation can result in funding shortfalls, contract modifications, or manpower reallocation.

Determining DoD SCADA vulnerability can be very difficult. Many limitations and operational restrictions can be imposed to DoD SCADA security and vulnerability assessments.   Future work can focus on developing relevant metrics and sound methodologies to assess operational SCADA systems.

Appendix A: CIP Evolution

CIP in the 80’s

In the 1980’s critical infrastructure was considered as public works and transportation, its protection was important because the services that they provided “formed the underpinnings of the nation’s defense, a strong economy, and our health and safety (Moteff and Parfomak, 2004).”

The CBO, in 1983 defined infrastructures as facilities with “the common characteristics of capital intensiveness and high public investment at all levels of government. They are, moreover, directly critical to activity in the nation’s economy (CBO, 1983).” The CBO included highways, public transit systems, wastewater treatment works, water resources, air traffic control, airports, and municipal water supply in this category (Moteff and Parfomak, 2004).

CIP in the 90’s

In 1996, President Clinton signed Executive Order 13010 categorizing critical infrastructure as “…so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the Unites States (Papa and Shenoi, 2008).” E.O. 13010 went further, by prioritizing particular infrastructure sectors, and specific assets within those sectors, on the basis of national importance (Moteff and Parfomak, 2004).

On this decade, concerns about terrorism lead to serious critical infrastructure efforts (Papa and Shenoi, 2008). Reflecting new realities, a key development on this decade was the inclusion of the term “cyber” to the definition of critical infrastructures.

In 1998, Presidential Decision Directive (PDD)-63 defines “critical” infrastructures as “those physical and cyber-based systems essential to the minimum operations of the economy and government (Moteff and Parfomak, 2004).”

CIP in the 2000’s

Changes resulting from the terrorist attacks of September 11, 2001 characterized this decade. New government organizations were created, the definition of critical infrastructure was expanded and new efforts to share and collaborate across private/government sectors were launched.

In 2001, President Bush signed Executive Order 13228, establishing the Office of Homeland Security and the Homeland Security Council (Moteff and Parfomak, 2004).

In 2002, The National Strategy for Homeland Security (NSHS), in addition to identifying critical infrastructure, it also introduces the concept of “key assets” as a subset of nationally important key resources (Moteff and Parfomak, 2004).

In 2003, The National Strategy for Physical Infrastructure Protection and Key Assets (NSPP) defines three categories of what it considers to be key assets:

(1) One category of key assets comprises the diverse array of national monuments, symbols, and icons that represent our Nation’s heritage, traditions and values, and political power.

(2) Another category of key assets includes facilities and structures that represent our national economic power and technological advancement.

(3) A third category of key assets includes such structures as prominent commercial centers, office buildings, and sports stadiums, where large numbers of people

regularly congregate to conduct business or personal transactions, shop, or enjoy a recreational pastime (Moteff and Parfomak 2004).

On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7) clarifying executive agency responsibilities for identifying, prioritizing and protecting critical infrastructure. HSPD-7 specifies a list of infrastructures; however, it leaves open the possibility that the list could be expanded. (Moteff and Parfomak, 2004).

Appendix B: DoD IA Definition of Information Systems Categories

-Automated Information System (AIS) Application: *“An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., integrated Consumable Items Support (ICIS)); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System (GCCS), Defense Messaging System (DMS))* (DoDI 8500.2, 2003).

- Enclave: *“Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers”* (DoDI 8500.2, 2003).

- Outsourced IT-based Process: *“For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations”* (DoDI 8500.2, 2003).

- Platform IT Interconnection (PIT):   *“For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has* *readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric"* (DoDI 8500.2, 2003).

Appendix C: Federal Government IA Documents (Abrams, 2007)

The following US government documents help define the cyber security environment. Regulations and guidance may not always be consistent. This list is not exhaustive. Other federal laws, regulations, and guidance not listed here may apply. Many organizations are governed by legislation that specifically applies to that organization (Abrams, 2007). Note: Attachment was compiled from MITRE Technical Report MTR070050.

Federal Laws and Regulations

- Public Law 107-347, Federal Information Security Management Act of 2002, December 17, 2002.
- Public Law 107-296, Critical Information Infrastructure Act of 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996.
- Public Law 99-474, The Computer Fraud and Abuse Act.
- 5 United States Code (U.S.C.) Section 552, "The Privacy Act of 1974."
- 44 U.S.C. Chapter 35, "Coordination of Federal Information Policy."
- United States Code of Federal Regulations (CFR) 29, Department of Homeland Security, "Procedures for Handling Critical Infrastructure Information."

Executive Orders

- Executive Order 12472, Assignment of National Security and Emergency Preparedness

Telecommunications Functions, April 3, 1984.

- Executive Order 13011, Federal Information Technology, July 16, 1996.

- Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001.
- PDD-63, Protecting America's Critical Infrastructures, May 22, 1998.
- Homeland Security Presidential Directive-3 (HSPD-3), Homeland Security Advisory System, March 11, 2002.

Office of Management and Budget

- OMB Circular Number A-130, *Management of Federal Information Resources*, February 8, 1996.
- OMB Circular Number A-123, *Management Accountability and Control*, revised June 21, 1999.
- OMB Circular A-11, *Preparation, Submission, Execution of Budgets*, July 16, 2004.
- OMB Memorandum M-00-10, *Procedures and Guidelines on Implementing the Government Paperwork Elimination Act*, April 25, 2002.
- PDD 12, *Security Awareness and Reporting of Foreign Contacts*, August 5, 1993.
- OMB Guide, *Evaluating Information Technology Investments*; http://www.whitehouse.gov/omb/inforeg/infotech.html, February 2, 2006

Department of Homeland Security (DHS)

- Homeland Security Presidential Directive (HSPD), DHS Policy Directive 3, *Homeland Security Advisory System*, March 11, 2002.
- HSPD, DHS Policy Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.

- HSPD, DHS Policy Directive 12, *Common Identification Standard for Federal Employees and Contractors*, August 24, 2004.

Department of Commerce (DOC)

- FIPS 140-2, *Security requirements for Cryptographic Modules*, May 2001.
- FIPS 180-2, *Secure Hash Standard (SHS),* August 2002, change notice February 2004.
- FIPS 186-2, *Digital Signature Standard (DSS),* January 2000.
- FIPS 188, *Standard Security Labels for Information Transfer*, September 1994.
- FIPS 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994
- FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC),* March 2002.
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

NIST

- SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995.
- SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995.
- SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

- SP 800-15, *Minimum Interoperability Specification for PKI Components (MISPC), Version 1*, September 1997.
- SP 800-16, *Information Technology Security Training Requirements: A Roleand Performance-Based Model*, April 1998.
- SP 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998.
- SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.
- SP 800-19, *Mobile Agent Security*, October 1999.
- SP 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TDEA): Requirements and Procedures*, October 1999, revised April 2000.
- SP 800-21-1, *Guideline for Implementing Cryptography in the Federal Government, Second edition*, December 2005.
- SP 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, October 2000, revised: May 15, 2001.
- SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.
- SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000.
- SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.
- SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

- SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A June 2004.
- SP 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.
- SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.
- SP 800-31, *Intrusion Detection Systems (IDS)*, November 2001.
- SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.
- SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.
- SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
- SP 800-35, *Guide to Information Technology Security Services*, October 2003.
- SP 800-36, *Guide to Selecting Information Security Products*, October 2003.
- SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004.
- SP 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.
- SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.
- SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004.

- SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*, draft April 20, 2006.
- SP 800-40, *Procedures for Handling Security Patches*, September 2002.
- SP 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002.
- SP 800-42, *Guideline on Network Security Testing*, October 2003.
- SP 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002.
- SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002.
- NIST SP 800-45, *Guidelines on Electronic Mail Security*, September 2002.
- SP 800-46, *Security for Telecommuting and Broadband Communications*, August 2002.
- SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002.
- SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, November 2002.
- SP 800-49, *Federal S/MIME V3 Client Profile*, November 2002.
- SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.
- SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.
- SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005.

- SP 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.
- SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, draft May 4, 2006.
- SP 800-54, *Border Gateway Protocol Security*, draft September 26, 2006.
- SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.
- SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2006.
- SP 800-57, *Recommendation on Key Management*, August 2005.
- SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.
- SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, August 2003.
- SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security System*, August 2003.
- SP 800-61, *Computer Security Incident Handling Guide*, January 2004.
- SP 800-63, Version 1.0.1, *Electronic Authentication Guideline*, September 2004.
- SP 800-64, *Security Considerations in the Information System Development Life Cycle*, rev 1 June 2004.
- SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.
- SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005.

•SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004.

• SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005.

• SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006.

• SP 800-70, *The NIST Security Configuration Checklists Program*, May 2005.

• SP 800-72, *Guidelines on PDA Forensics*, November 2004.

• SP 800-73, *Interfaces for Personal Identity Verification*, April 2005.

• SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, draft September 14, 2006.

• SP 800-77, *Guide to IPSec VPNs*, December 2005.

• SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005.

• SP 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005.

• SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006.

• SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, draft September 2006.

• SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

• SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

• SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines*

(SP800-73 compliance), April 2006.

- SP 800-85B, *PIV Data Model Conformance Test Guidelines*, July 2006.
- SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.
- SP 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, October 2005 (document updated January 17, 2006).
- SP 800-88, *Guidelines for Media Sanitization*, September 2006.
- SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006.
- SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2006.
- SP 800-92, *Guide to Computer Security Log Management*, September 2006.
- SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, draft August 31, 2006.
- SP 800-95, *Guide to Secure Web Services*, draft August 31, 2006.
- SP 800-96, *PIV Card/Reader Interoperability Guidelines*, September 2006.
- SP 800-97, *Guide to IEEE 802.11i: Robust Security Networks*, draft June 5, 2006.
- SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, draft September 26, 2006.
- SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.
- SP 800-101, *Guidelines on Cell Phone Forensics*, draft August 31, 2006.

Appendix D: NIST SP 800-82 ICS Controls

NIST SP 800-82	
6.1.1	Risk Assessment (Page 6-2)
6.1.2	Planning ((Page 6-3)
6.1.3	System and Service Acquisition (Page 6-4)
6.1.4	Certification, Accreditation, and Security Assessments (Page 6-5)
6.2.1	Personnel Security (Page 6-7)
6.2.2	Physical & Environmental Protection, (Page 6-7)
6.2.2.1	Control Center/Control Room (Page 6-10)
6.2.2.2	Portable Devices (Page 6-10)
6.2.2.3	Cabling (Page 6-10)
6.2.3	Contingency Planning (Page 6-11)
6.2.3.2	Disaster Recovery Planning (Page 6-12)
6.2.4	Configuration Management (Page 6-13)
6.2.6	System and Information Integrity (Page 6-14)
6.2.6.1	Malicious Code Detection (Page 6-15)
6.2.6.2	Intrusion Detection and Prevention (Page 6-15)
6.2.6.3	Patch Management (Page 6-16)
6.2.7	Media Protection (Page 6-18)
6.2.8	Incident Response (Page 6-18)
6.2.9	Awareness and Training (Page 6-21)
6.3.1	Identification and Authentication (Page 6-22)
6.3.1.1	Password Authentication (Page 6-23)
6.3.1.3	Physical Token Authentication (Page 6-25)
6.3.2.1	Role-Based Access Control (Page 6-27)
6.3.2.2	Web Servers (Page 6-28)
6.3.2.3	Virtual Local Area Network (Page 6-28)
6.3.2.4	Dial-up Modems (Page 6-29)
6.3.2.5	Wireless (Page 6-30)

6.3.3	Audit and Accountability (Page 6-31)
6.3.4.1	Encryption (Page 6-33)
6.3.4.2	Virtual Private Network (VPN) (Page 6-34)

Appendix E: DoD IA Controls

Control Number	Control Name	Subject Area	DoD IA Control Description (DoD 8500.2)
COAS-1	Alternate Site Designation	Continuity	An alternate site is identified that permits the partial restoration of mission or business essential functions.
COAS-2	Alternate Site Designation	Continuity	An alternate site is identified that permits the restoration of all mission or business essential functions.
COBR-1	Protection of Backup and Restoration Assets	Continuity	Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.
CODB-1	Data Backup Procedures	Continuity	Data backup is performed at least weekly.
CODB-2	Data Backup Procedures	Continuity	Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.
CODB-3	Data Backup Procedures	Continuity	Data backup is accomplished by maintaining a redundant secondary system, not co-located, that can be activated without loss of data or disruption to the operation.
CODP-1	Disaster and Recovery Planning	Continuity	A disaster plan exists that provides for the partial resumption of mission or business essential functions within 5 days of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)
CODP-2	Disaster and Recovery Planning	Continuity	A disaster plan exists that provides for the resumption of mission or business essential functions within 24 hours of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)
CODP-3	Disaster and Recovery Planning	Continuity	A disaster plan exists that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)
COEB-1	Enclave Boundary Defense	Continuity	Enclave boundary defense at the alternate site provides security measures equivalent to the primary site.
COEB-2	Enclave Boundary Defense	Continuity	Enclave boundary defense at the alternate site must be configured identically to that of the primary site.
COED-1	Scheduled Exercises and	Continuity	The continuity of operations or disaster recovery plans are exercised annually.

	Drills		
COED-2	Scheduled Exercises and Drills	Continuity	The continuity of operations or disaster recovery plans or significant portions are exercised semi-annually.
COEF-1	Identification of Essential Functions	Continuity	Mission and business essential functions are identified for priority restoration planning.
COEF-2	Identification of Essential Functions	Continuity	Mission and business-essential functions are identified for priority restoration planning along with all assets supporting mission or business-essential functions (e.g., computer-based services, data and applications, communications, physical infrastructure).
COMS-1	Maintenance Support	Continuity	Maintenance support for key IT assets is available to respond within 24 hours of failure.
COMS-2	Maintenance Support	Continuity	Maintenance support for key IT assets is available to respond 24 X 7 immediately upon failure.
COPS-1	Power Supply	Continuity	Electrical power is restored to key IT assets by manually activated power generators upon loss of electrical power from the primary source.
COPS-2	Power Supply	Continuity	Electrical systems are configured to allow continuous or uninterrupted power to key IT assets. This may include an uninterrupted power supply coupled with emergency generators.
COPS-3	Power Supply	Continuity	Electrical systems are configured to allow continuous or uninterrupted power to key IT assets and all users accessing the key IT assets to perform mission or business-essential functions. This may include an uninterrupted power supply coupled with emergency generators or other alternate power source.
COSP-1	Spares and Parts	Continuity	Maintenance spares and spare parts for key IT assets can be obtained within 24 hours of failure.
COSP-2	Spares and Parts	Continuity	Maintenance spares and spare parts for key IT assets are available 24 X 7 immediately upon failure.
COSW-1	Backup Copies of Critical SW	Continuity	Back-up copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software.
COTR-1	Trusted Recovery	Continuity	Recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place.
DCAR-1	Procedural Review	Security Design and Configuration	An *annual* IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.
DCAS-1	Acquisition Standards	Security Design and Configuration	The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-

			approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources - the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation (See also DCSR-1).
DCBP-1	Best Security Practices	Security Design and Configuration	The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics.
DCCB-1	Control Board	Security Design and Configuration	All DoD information systems are under the control of a chartered configuration control board that meets regularly according to DCPR-1.
DCCB-2	Control Board	Security Design and Configuration	All information systems are under the control of a chartered Configuration Control Board that meets regularly according to DCPR-1. The IAM is a voting member of the CCB.
DCCS-1	Configuration Specifications	Security Design and Configuration	A DoD reference document, such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a DoD reference document is not available, the following are acceptable in descending order as available: (1) Commercially accepted practices (e.g., SANS); (2) Independent testing results (e.g., ICSA); or (3) Vendor literature.
DCCS-2	Configuration Specifications	Security Design and Configuration	A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a DoD reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a Departmental reference guide.
DCCT-1	Compliance Testing	Security Design and Configuration	A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.
DCDS-1	Dedicated IA Services	Security Design and Configuration	Acquisition or outsourcing of dedicated IA services such as incident monitoring, analysis and response; operation of IA devices such as

			firewalls; or key management services are supported by a formal risk analysis and approved by the DoD Component CIO.
DCFA-1	Functional Architecture for AIS Applications	Security Design and Configuration	For AIS applications, a functional architecture that identifies the following has been developed and is maintained: - all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface - user roles required for access control and the access privileges assigned to each role (See ECAN) - unique security requirements (e.g., encryption of key data elements at rest) - categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA) - restoration priority of subsystems, processes, or information (See COEF).
DCHW-1	HW Baseline	Security Design and Configuration	A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.
DCID-1	Interconnection Documentation	Security Design and Configuration	For AIS applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements. For enclaves, a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.
DCII-1	IA Impact Assessment	Security Design and Configuration	Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.
DCIT-1	IA for IT Services	Security Design and Configuration	Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.
DCMC-1	Mobile Code	Security Design and Configuration	The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements: 1. Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is not used. 2. Category 1 mobile code is signed with a DoD-approved PKI code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.

			3. Category 2 mobile code, which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used. 4. Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME, code is signed with a DoD-approved code signing certificate). 5. Category 3 mobile code may be used. 6. All DoD workstation and host software are configured, to the extent possible, to prevent the download and execution of mobile code that is prohibited. 7. The automatic execution of all mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments.
DCNR-1	Non-repudiation	Security Design and Configuration	NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.
DCPA-1	Partitioning the Application	Security Design and Configuration	User interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods, as appropriate.
DCPB-1	IA Program and Budget	Security Design and Configuration	A discrete line item for Information Assurance is established in programming and budget documentation.
DCPD-1	Public Domain Software Controls	Security Design and Configuration	Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.
DCPP-1	Ports, Protocols,	Security	DoD information systems comply with DoD ports,

	and Services	Design and Configuration	protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.
DCPR-1	CM Process	Security Design and Configuration	A configuration management (CM) process is implemented that includes requirements for: 1. Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation; 2. A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems; 3. A testing process to verify proposed configuration changes prior to implementation in the operational environment; and 4. A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.
DCSD-1	IA Documentation	Security Design and Configuration	All appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup or emergency response).
DCSL-1	System Library Management Controls	Security Design and Configuration	System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.
DCSP-1	Security Support Structure Partitioning	Security Design and Configuration	The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process.
DCSQ-1	Software Quality	Security Design and Configuration	Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.
DCSR-1	Specified	Security	At a minimum, basic-robustness COTS IA and IA-

	Robustness - Basic	Design and Configuration	enabled products are used to protect publicly released information from malicious tampering or destruction and ensure its availability. The basic-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Basic Robustness published under the IATF.
DCSR-2	Specified Robustness - Medium	Security Design and Configuration	At a minimum, medium-robustness COTS IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system. The medium-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Medium Robustness published under the IATF. *COTS IA and IA-enabled IT products used for access control, data separation, or privacy on sensitive systems already protected by approved medium-robustness products, at a minimum, satisfy the requirements for basic robustness.* If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.
DCSR-3	Specified Robustness – High	Security Design and Configuration	Only high-robustness GOTS or COTS IA and IA-enabled IT products are used to protect *classified information when the information transits networks that are at a lower classification level than the information being transported*. High-robustness products have been evaluated by NSA or in accordance with NSA-approved processes. COTS IA and IA-enabled IT products used for access control, data separation or privacy on classified systems already protected by approved high-robustness products at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.
DCSS-1	System State Changes	Security Design and Configuration	System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state.
DCSS-2	System State Changes	Security Design and Configuration	System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. Tests are provided and periodically run to ensure the integrity of the system state.
DCSW-1	SW Baseline	Security Design and Configuration	A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.

EBBD-1	Boundary Defense	Enclave Boundary Defense	Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, and Internet access is permitted from a demilitarized zone (DMZ) that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means. All Internet access points are under the management and control of the enclave. Internet access is permitted from a demilitarized zone (DMZ) that meets the DoD requirement that such contacts are isolated from other DoD systems by physical or technical means. All Internet access points are under the management and control of the enclave.
EBBD-2	Boundary Defense	Enclave Boundary Defense	Boundary defense mechanisms, to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries, or at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.
EBBD-3	Boundary Defense	Enclave Boundary Defense	Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, and at layered or internal enclave boundaries and key points in the network as required. All Internet access is prohibited.
EBCR-1	Connection Rules	Enclave Boundary Defense	The DoD information system is compliant with established DoD connection rules and approval processes.
EBPW-1	Public WAN Connection	Enclave Boundary Defense	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ).
EBRP-1	Remote Access for Privileged Functions	Enclave Boundary Defense	Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/IAO reviews the log for every remote session.
EBRU-1	Remote Access for User Functions	Enclave Boundary Defense	All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session-level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g.,

			Internet address, dial-up connection telephone number) is protected.
EBVC-1	VPN Controls	Enclave Boundary Defense	All VPN traffic is visible to network intrusion detection systems (IDS).
ECAD-1	Affiliation Display	Enclave Computing Environment	To help prevent inadvertent disclosure of controlled information, all contractors are identified by the inclusion of the abbreviation "ctr" and all foreign nationals are identified by the inclusion of their two character country code in: - DoD user e-mail addresses (e.g., john.smith.ctr@army.mil orjohn.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor <john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both (e.g.,john.smith.ctr.uk@army.mil). Country codes and guidance regarding their use are in FIPS 10-4.
ECAN-1	Access for Need-to-Know	Enclave Computing Environment	Access to all DoD information (classified, sensitive, and public) is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls. Access controls are established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access: 1. Open access to general information that is made available to all DoD authorized users with network access. Access does not require an audit transaction. 2. Controlled access to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction.
ECAR-1	Audit Record Content – Public Systems	Enclave Computing Environment	Audit records include: · User ID. · Successful and unsuccessful attempts to access security files. · Date and time of the event. · Type of event.
ECAR-2	Audit Record Content – Sensitive Systems	Enclave Computing Environment	Audit records include: · User ID. · Successful and unsuccessful attempts to access security files. · Date and time of the event. · Type of event. · Success or failure of event.

			· Successful and unsuccessful logons. · Denial of access resulting from excessive number of logon attempts. · Blocking or blacklisting a user ID, terminal or access port and the reason for the action. · Activities that might modify, bypass, or negate safeguards controlled by the system.
ECAR-3	Audit Record Content – Classified Systems	Enclave Computing Environment	Audit records include: · User ID. · Successful and unsuccessful attempts to access security files. · Date and time of the event. · Type of event. · Success or failure of event. · Successful and unsuccessful logons. · Denial of access resulting from excessive number of logon attempts. · Blocking or blacklisting a user ID, terminal or access port, and the reason for the action. · Activities that might modify, bypass, or negate safeguards controlled by the system. · Data required auditing the possible use of covert channel mechanisms. · Privileged activities and other system-level access. · Starting and ending time for access to the system. · Security relevant actions associated with periods processing or the changing of security labels or categories of information.
ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	Enclave Computing Environment	Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures.
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	Enclave Computing Environment	An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.
ECCD-1	Changes to Data	Enclave Computing Environment	Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel.
ECCD-2	Changes to Data	Enclave Computing Environment	Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel. Access and changes to the data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content.
ECCM-1	COMSEC	Enclave Computing Environment	COMSEC activities comply with DoD Directive C-5200.5.

ECCR-1	Encryption for Confidentiality (Data at Rest)	Enclave Computing Environment	If required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.
ECCR-2	Encryption for Confidentiality (Data at Rest)	Enclave Computing Environment	If required by the information owner, NIST-certified cryptography is used to encrypt stored classified non-SAMI information.
ECCR-3	Encryption for Confidentiality (Data at Rest)	Enclave Computing Environment	If a classified enclave contains SAMI and is accessed by individuals lacking an appropriate clearance for SAMI, then NSA-approved cryptography is used to encrypt all SAMI stored within the enclave.
ECCT-1	Encryption for Confidentiality (Data at Transmit)	Enclave Computing Environment	Enclave Computing Environment
ECCT-2	Encryption for Confidentiality (Data at Transmit)	Enclave Computing Environment	Classified data transmitted through a network that is cleared to a lower level than the data being transmitted are separately encrypted using NSA-approved cryptography (See also DCSR-3).
ECDC-1	Data Change Controls	Enclave Computing Environment	Transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents.
ECIC-1	Interconnections among DoD Systems and Enclaves	Enclave Computing Environment	Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks. Controlled interfaces are addressed in separate guidance.
ECID-1	Host Based IDS	Enclave Computing Environment	Host-based intrusion detection systems are deployed for major applications and for network management assets, such as routers, switches, and domain name servers (DNS).
ECIM-1	Instant Messaging	Enclave Computing Environment	Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems. Both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary. Note: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.
ECLC-1	Audit of Security Label Changes	Enclave Computing Environment	The system automatically records the creation, deletion, or modification of confidentiality or integrity labels, if required by the information owner.
ECLO-1	Logon	Enclave Computing Environment	Successive logon attempts are controlled using one or more of the following: · Access is denied after multiple unsuccessful logon attempts. · The number of access attempts in a given

			period is limited. · A time-delay control system is employed. If the system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions.
ECLO-2	Logon	Enclave Computing Environment	Successive logon attempts are controlled using one or more of the following: · Access is denied after multiple unsuccessful logon attempts. · The number of access attempts in a given period is limited. · A time-delay control system is employed. If the system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions. Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon.
ECLP-1	Least Privilege	Enclave Computing Environment	Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.
ECML-1	Marking and Labeling	Enclave Computing Environment	Information and DoD information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents such as DoD 5200.1R. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions.
ECMT-1	Conformance Monitoring and Testing	Enclave Computing Environment	Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.
ECMT-2	Conformance Monitoring and Testing	Enclave Computing Environment	Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to

			ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.
ECND-1	Network Device Controls	Enclave Computing Environment	An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA).
ECND-2	Network Device Controls	Enclave Computing Environment	An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA). Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested.
ECNK-1	Encryption for Need-To-Know	Enclave Computing Environment	Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality – data in transit).
ECNK-2	Encryption for Need-To-Know	Enclave Computing Environment	SAMI information in transit through a network at the same classification level is encrypted using NSA-approved cryptography. This is to separate it for need-to-know reasons. This is in addition to ECCT (encryption for confidentiality – data in transit).
ECPA-1	Privileged Account Control	Enclave Computing Environment	All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web-administration). The IAM tracks privileged role assignments.
ECPC-1	Production Code Change Controls	Enclave Computing Environment	Application programmer privileges to change production code and data are limited and are periodically reviewed.
ECPC-2	Production Code Change Controls	Enclave Computing Environment	Application programmer privileges to change production code and data are limited and reviewed every 3 months.
ECRC-1	Resource Control	Enclave Computing Environment	All authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the

			system. There is absolutely no residual data from the former object.
ECRG-1	Audit Reduction and Report Generation	Enclave Computing Environment	Tools are available for the review of audit records and for report generation from audit records.
ECRR-1	Audit Record Retention	Enclave Computing Environment	If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.
ECSC-1	Security Configuration Compliance	Enclave Computing Environment	For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.
ECSD-1	Software Development Change Controls	Enclave Computing Environment	Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented.
ECSD-2	Software Development Change Controls	Enclave Computing Environment	Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented. Change controls include review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.
ECTB-1	Audit Trail Backup	Enclave Computing Environment	The audit records are backed up not less than weekly onto a different system or media than the system being audited.
ECTC-1	Tempest Controls	Enclave Computing Environment	Measures to protect against compromising emanations have been implemented according to DoD Directive S-5200.19.
ECTM-1	Transmission Integrity Controls	Enclave Computing Environment	Good engineering practices with regards to the integrity mechanisms of COTS, GOTS and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs).
ECTM-2	Transmission Integrity Controls	Enclave Computing Environment	Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).
ECTP-1	Audit Trail Protection	Enclave Computing Environment	The contents of audit trails are protected against unauthorized access, modification or deletion.
ECVI-1	Voice-over-IP (VoIP) Protection	Enclave Computing Environment	Voice over Internet Protocol (VoIP) traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within DoD information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary. Note: This does not include

			VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.
ECVP-1	Virus Protection	Enclave Computing Environment	All Servers, workstations and mobile computing devices (i.e. laptop, PDAs) implement virus protection that includes a capability for automatic updates.
ECWM-1	Warning Message	Enclave Computing Environment	All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.
ECWN-1	Wireless Computing and Network	Enclave Computing Environment	Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy, as issued. (See also ECCT). Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are normally disabled by changing factory defaults, settings or configurations prior to issue to end users. Wireless computing and networking capabilities are not independently configured by end users.
IAAC-1	Account Control	Identification and Authentication	A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.
IAGA-1	Group Authentication	Identification and Authentication	Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA).
IAIA-1	Individual Identification and Authentication	Identification and Authentication	DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are

			implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.
IAIA-2	Individual Identification and Authentication	Identification and Authentication	DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user logon ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement these measures to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Multiple forms of certification of individual identification such as a documentary evidence or a combination of documents and biometrics are presented to the registration authority. Additionally, to the extent capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse, and processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password). All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.
IAKM-1	Key Management	Identification and Authentication	Symmetric Keys are produced, controlled, and distributed using NIST-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Class 3 certificates or pre-placed keying material.
IAKM-2	Key Management	Identification and Authentication	Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD

			PKI Medium Assurance or High Assurance certificates and hardware security tokens that protect the user's private key.
IAKM-3	Key Management	Identification and Authentication	Symmetric and asymmetric keys are produced, controlled and distributed using NSA-approved key management technology and processes.
IATS-1	Token and Certificate Standards	Identification and Authentication	Identification and authentication is accomplished using the DoD PKI Class 3 certificate and hardware security token (when available).
IATS-2	Token and Certificate Standards	Identification and Authentication	Identification and authentication is accomplished using the DoD PKI Class 3 or 4 certificate and hardware security token (when available) or an NSA-certified product.
PECF-1	Access to Computing Facilities	Physical and Environmental	Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release.
PECF-2	Access to Computing Facilities	Physical and Environmental	Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.
PECS-1	Clearing and Sanitizing	Physical and Environmental	All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense according to DoD 5200.1-R and ASD(C3I) Memorandum, dated June 4, 2001, subject: "Disposition of Unclassified DoD Computer Hard Drives."
PECS-2	Clearing and Sanitizing	Physical and Environmental	All documents, equipment, and machine-readable media containing classified data are cleared and sanitized before being released outside its security domain according to DoD 5200.1-R.
PEDD-1	Destruction	Physical and Environmental	All documents, machine-readable media, and equipment are destroyed using procedures that comply with DoD policy (e.g., DoD 5200.1-R).
PEDI-1	Data Interception	Physical and Environmental	Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.
PEEL-1	Emergency Lighting	Physical and Environmental	An automatic emergency lighting system is installed that covers emergency exits and evacuation routes.
PEEL-2	Emergency Lighting	Physical and Environmental	An automatic emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes.
PEFD-1	Fire Detection	Physical and Environmental	Battery-operated or electric stand-alone smoke detectors are installed in the facility.
PEFD-2	Fire Detection	Physical and Environmental	A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system.
PEFI-1	Fire Inspection	Physical and Environmental	Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.

PEFS-1	Fire Suppression	Physical and Environmental	Handheld fire extinguishers or fixed fire hoses are available should an alarm be sounded or a fire be detected.
PEFS-2	Fire Suppression	Physical and Environmental	A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke, or particles.
PEHC-1	Humidity Controls	Physical and Environmental	Humidity controls are installed that provide an alarm of fluctuations potentially harmful to personnel or equipment operation; adjustments to humidifier/de-humidifier systems may be made manually.
PEHC-2	Humidity Controls	Physical and Environmental	Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.
PEMS-1	Master Power Switch	Physical and Environmental	A **master power switch** or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and **protected by a cover to prevent accidental shut-off**.
PEPF-1	Physical Protection of Facilities	Physical and Environmental	Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours.
PEPF-2	Physical Protection of Facilities	Physical and Environmental	Every physical access point to facilities housing workstations that process or display classified information is guarded or alarmed 24 X 7. Intrusion alarms are monitored. Two (2) forms of identification are required to gain access to the facility (e.g., ID badge, key card, cipher PIN, biometrics). A visitor log is maintained.
PEPS-1	Physical Security Testing	Physical and Environmental	A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.
PESL-1	Screen Lock	Physical and Environmental	Unless there is an overriding technical or operational problem, workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was previously visible on the screen. Such a capability is enabled either by explicit user action or a specified period of workstation inactivity (e.g., 15 minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator. A screen lock function is not considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).
PESP-1	Workplace Security Procedures	Physical and Environmental	Procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.

PESS-1	Storage	Physical and Environmental	Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.
PETC-1	Temperature Controls	Physical and Environmental	Temperature controls are installed that provide an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected; adjustments to heating or cooling systems may be made manually.
PETC-2	Temperature Controls	Physical and Environmental	Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.
PETN-1	Environmental Control Training	Physical and Environmental	Employees receive initial and periodic training in the operation of environmental controls.
PEVC-1	Visitor Control to Computing Facilities	Physical and Environmental	Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.
PEVR-1	Voltage Regulators	Physical and Environmental	Automatic voltage control is implemented for key IT assets.
PRAS-1	Access to Information	Personnel	Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.
PRAS-2	Access to Information	Personnel	Individuals requiring access to classified information are processed for access authorization in accordance with DoD personnel security policies.
PRMP-1	Maintenance Personnel	Personnel	Maintenance is performed only by authorized personnel. The process for determining authorization and the list of authorized maintenance personnel is documented.
PRMP-2	Maintenance Personnel	Personnel	Maintenance is performed only by authorized personnel. The process for determining authorization and the list of authorized maintenance personnel is documented. Except as authorized by the DAA, personnel who perform maintenance on classified DoD information systems are cleared to the highest level of information on the system. Cleared personnel who perform maintenance on a classified DoD information system require an escort unless they have authorized access to the computing facility and the DoD information system. If uncleared or lower-cleared personnel are employed, a fully cleared and technically qualified escort monitors and records all activities in a maintenance log. The level of detail required in the maintenance log is determined by the IAM. All maintenance personnel comply with DAA requirements for U.S. citizenship, which are explicit for all classified systems.
PRNK-1	Access to Need-to-Know Information	Personnel	Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel

			security criteria (e.g., IT position sensitivity background investigation requirements outlined in DoD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the information owner.
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	Personnel	A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.
PRTN-1	Information Assurance Training	Personnel	A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA-related plans such as incident response, configuration management and COOP or disaster recovery.
VIIR-1	Incident Response Planning	Vulnerability and Incident Management	An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2 and CJCS Instruction 6510.01D, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually.
VIIR-2	Incident Response Planning	Vulnerability and Incident Management	An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2 and CJCS Instruction 6510.01D, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least every 6 months.
VIVM-1	Vulnerability Management	Vulnerability and Incident Management	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL)

			to test for the presence of vulnerabilities.

Appendix F: IA Control Correlation

Correlation Code 8

Strength Correlation					
	8. NIST requirement and DoD IA control are equivalent.				
	NIST		DoD IA Controls		R Rank
	Which security controls have the greatest impact on the security of ICS/SCADA systems (rank order- # 1 is the most important)?				
	6.1.3	System and Services Acquisition	DCAS-1	Acquisition Standards	
	6.2.2	Physical and Environmental Protection	COPS-1	Power Supply	
	6.2.2	Physical and Environmental Protection	PECF-1	Access to Computing Facilities	
	6.2.2.1	Control Center/Control Room	COAS-2	Alternate Site Designation	
	6.2.2.1	Control Center/Control Room	PECF-1	Access to Computing Facilities	
	6.2.3	Contingency Planning	COAS-1	Alternate Site Designation	
	6.2.3	Contingency Planning	COBR-1	Protection of Backup and Restoration Assets	
	6.2.3	Contingency Planning	CODB-1	Data Backup Procedures	
	6.2.3.2	Disaster Recovery Planning	COBR-1	Protection of Backup and Restoration Assets	
	6.2.3.2	Disaster Recovery Planning	CODB-1	Data Backup Procedures	
	6.2.4	Configuration Management	DCII-1	IA Impact Assessment	
	6.2.4	Configuration Management	DCIT-1	IA for IT Services	
	6.2.6.1	Malicious Code Detection	ECVP-1	Virus Protection	
	6.2.6.3	Patch Management	DCCT-1	Compliance Testing	
	6.2.8	Incident Response	PRTN-1	Information Assurance Training	
	6.2.9	Awareness and Training	PETN-1	Environmental Control Training	
	6.3.3	Audit and Accountability	ECRG-1	Audit Reduction and Report Generation	
	6.3.4.1	Encryption	DCNR-1	Non-repudiation	
	6.3.4.1	Encryption	IAKM-3	Key Management	

Correlation Code 9

	Strength Correlation				
	9. NIST requirement is more specific than the DoD IA control.				
	NIST			DoD IA Controls	R Rank
	Which security controls have the greatest impact on the security of ICS/SCADA systems (rank order- # 1 is the most important)?				
	6.2.3.4	Dial-Up Modems	EBRP-1	Remote Access for Privileged Functions	
	6.3.1.1	Password Authentication	IAIA-1	Individual Identification and Authentication	

Correlation Code 17

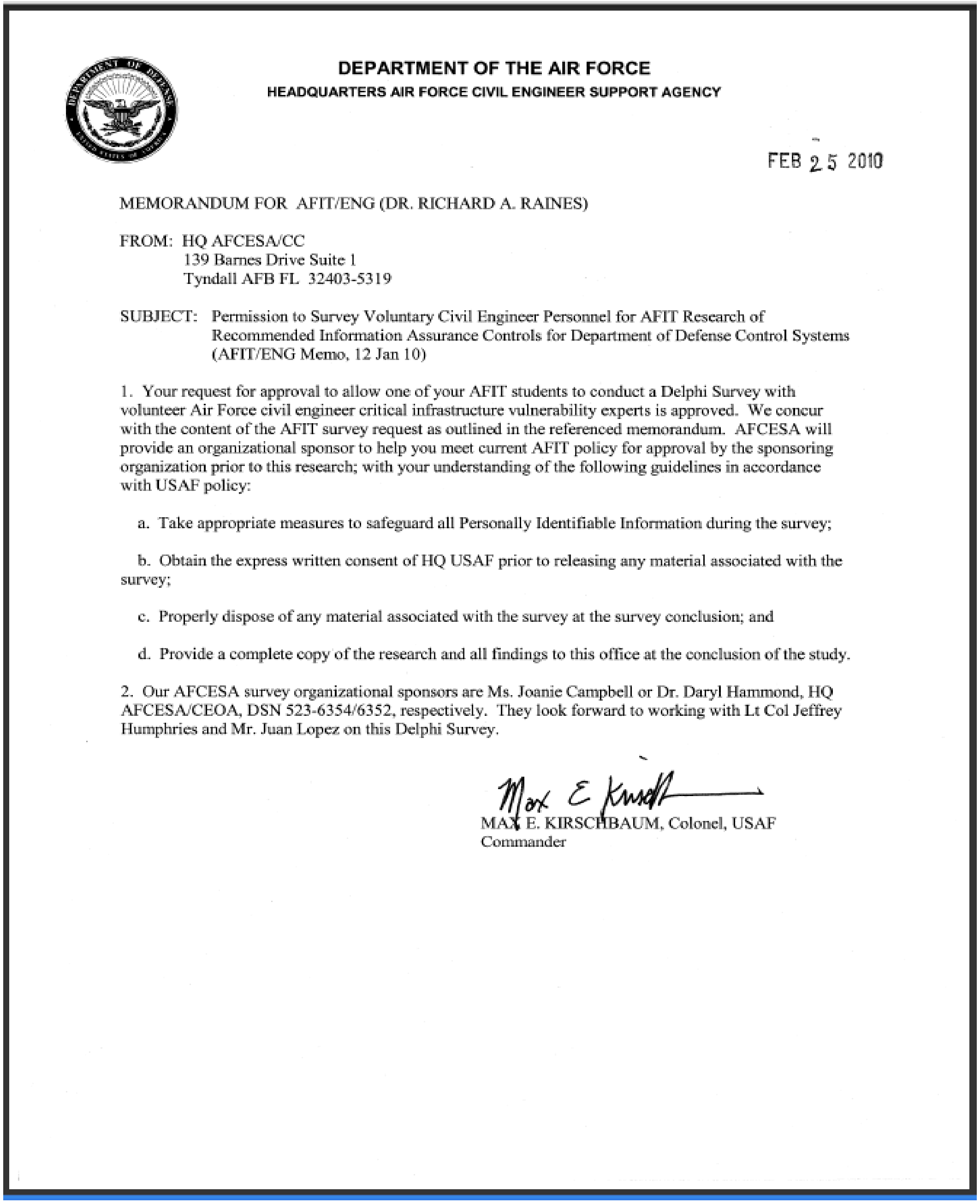
Strength Correlation				
17. NIST requirement is less specific than the DoD IA control.				
NIST		DoD IA Controls		Rank
Which security controls have the greatest impact on the security of ICS/SCADA systems (rank order- # 1 is the most important)?				
6.1.1	Risk Assessment	VIVM-1	Vulnerability Management	
6.1.2	Planning	DCSD-1	IA Documentation	
6.2.2	Physical and Environmental Protection	PRAS-1	Access to Information	
6.2.1	Personnel Security	PRNK-1	Access to Need-to-Know Information	
6.2.1	Personnel Security	COPS-1	Power Supply	
6.2.2	Physical and Environmental Protection	ECND-1	Network Device Controls	
6.2.2	Physical and Environmental Protection	PECF-2	Access to Computing Facilities	
6.2.2	Physical and Environmental Protection	PEHC-1	Humidity Controls	
6.2.2	Physical and Environmental Protection	PEMS-1	Master Power Switch	
6.2.2	Physical and Environmental Protection	PEPF-1	Physical Protection of Facilities	
6.2.2	Physical and Environmental Protection	PESS-1	Storage	
6.2.2	Physical and Environmental Protection	PETC-1	Temperature Controls	
6.2.2.1	Control Center/Control Room	PECF-2	Access to Computing Facilities	
6.2.3	Contingency Planning	CODP-1	Disaster and Recovery Planning	
6.2.3	Contingency Planning	COEB-1	Enclave Boundary Defense	
6.2.3	Contingency Planning	COED-1	Scheduled Exercises and Drills	
6.2.3	Contingency Planning	COEF-1	Identification of Essential Functions	
6.2.3	Contingency Planning	COTR-1	Trusted Recovery	
6.2.3.2	Disaster Recovery Planning	CODP-1	Disaster and Recovery Planning	
6.2.3.2	Disaster Recovery Planning	COEB-1	Enclave Boundary Defense	
6.2.3.2	Disaster Recovery Planning	COED-1	Scheduled Exercises and Drills	
6.2.3.2	Disaster Recovery Planning	COEF-1	Identification of Essential Functions	
6.2.3.2	Disaster Recovery Planning	COMS-1	Maintenance Support	
6.2.4	Configuration Management	DCCB-1	Control Board	
6.2.4	Configuration Management	DCFA-1	Functional Architecture for AIS Applications	
6.2.4	Configuration Management	DCPD-1	Public Domain Software Controls	
6.2.4	Configuration Management	DCPR-1	CM Process	
6.2.4	Configuration Management	DCSQ-1	Software Quality	
6.2.4	Configuration Management	ECSD-1	Software Development Change Controls	
6.2.6	System and Information Integrity	DCPA-1	Partitioning the Application	
6.2.6	System and Information Integrity	DCSD-1	IA Documentation	
6.2.6.2	Intrusion Detection and Prevention	EBBD-1	Boundary Defense	
6.2.6.2	Intrusion Detection and Prevention	EBVC-1	VPN Controls	

	6.2.6.2	Intrusion Detection and Prevention	ECID-1	Host Based IDS	
	6.2.7	Media Protection	ECML-1	Marking and Labeling	
	6.2.7	Media Protection	PECS-1	Clearing and Sanitizing	
	6.2.7	Media Protection	PEDD-1	Destruction	
	6.2.7	Media Protection	PEDI-1	Data Interception	
	6.2.7	Media Protection	PESP-1	Workplace Security Procedures	
	6.2.7	Media Protection	PESS-1	Storage	
	6.2.8	Incident Response	VIIR-1	Incident Response Planning	
	6.2.8	Incident Response	VIVM-1	Vulnerability Management	
	6.3.1.3	Physical Token Authentication	IATS-1	Token and Certificate Standards	
	6.3.2.1	Role-Based Access Control (RBAC)	ECAN-1	Access for Need-to-Know	
	6.3.2.1	Role-Based Access Control (RBAC)	ECPA-1	Privileged Account Control	
	6.3.2.2	Web Servers	ECLP-1	Least Privilege	
	6.3.2.3	Virtual Local Area Network (Vlan)	DCPA-1	Partitioning the Application	
	6.3.2.4	Dial-Up Modems	EBRU-1	Remote Access for User Functions	
	6.3.2.5	Wireless	DCCS-1	Configuration Specifications	
	6.3.2.5	Wireless	ECWN-1	Wireless Computing and Network	
	6.3.3	Audit and Accountability	ECAR-1	Audit Record Content – Public Systems	
	6.3.3	Audit and Accountability	ECAT-1	Audit Trail, Monitoring, Analysis and Reporting	
	6.3.3	Audit and Accountability	ECCD-1	Changes to Data	
	6.3.3	Audit and Accountability	ECMT-1	Conformance Monitoring and Testing	
	6.3.3	Audit and Accountability	ECTB-1	Audit Trail Backup	
	6.3.3	Audit and Accountability	ECTP-1	Audit Trail Protection	
	6.3.4.1	Encryption	DCSR-1	Specified Robustness - Basic	
	6.3.4.1	Encryption	ECCR-1	Encryption for Confidentiality (Data at Rest)	
	6.3.4.1	Encryption	ECCT-1	Encryption for Confidentiality (Data at Transmit)	
	6.3.4.1	Encryption	ECNK-1	Encryption for Need-To-Know	
	6.3.4.1	Encryption	IAKM-1	Key Management	
	6.3.4.2	Virtual Private Network	DCSR-1	Specified Robustness - Basic	
	6.3.4.2	Virtual Private Network	EBRP-1	Remote Access for Privileged Functions	
	6.3.4.2	Virtual Private Network	EBRU-1	Remote Access for User Functions	
	6.3.4.2	Virtual Private Network	EBVC-1	VPN Controls	

Correlation Code 11

	Strength Correlation				
	11. NIST requirement has no counterpart in the DoD IA control.				
	NIST		DoD IA Controls		R Rank
	Which security controls have the greatest impact on the security of ICS/SCADA systems (rank order- # 1 is the most important)?				
	6.2.2	Physical and Environmental Protection	~PETS	Toxic Substance Controls	
	6.2.2.1	Control Center/Control Room	~PEBP	Blast Protection	
	6.2.2.2	Portable Devices	~PEAD	Access Control to IT Devices	
	6.2.2.3	Cabling	~PETP	Physical Protection of Transmition Medium	
	6.3.2.3	Virtual Local Area Network (Vlan)	`DCVP	Virtual Partitioning	
	6.3.2.1	Role-Based Access Control (RBAC)	ECLP	Enclave Computing Environment	
	6.3.2.2	Web Servers	EBRP	Enclave Boundary Defense	
	6.3.2.4	Dial-Up Modem	EBRP	Enclave Boundary Defense	

Appendix G: Survey Approval Letter



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE CIVIL ENGINEER SUPPORT AGENCY

FEB 25 2010

MEMORANDUM FOR AFIT/ENG (DR. RICHARD A. RAINES)

FROM: HQ AFCESA/CC
139 Barnes Drive Suite 1
Tyndall AFB FL 32403-5319

SUBJECT: Permission to Survey Voluntary Civil Engineer Personnel for AFIT Research of Recommended Information Assurance Controls for Department of Defense Control Systems (AFIT/ENG Memo, 12 Jan 10)

1. Your request for approval to allow one of your AFIT students to conduct a Delphi Survey with volunteer Air Force civil engineer critical infrastructure vulnerability experts is approved. We concur with the content of the AFIT survey request as outlined in the referenced memorandum. AFCESA will provide an organizational sponsor to help you meet current AFIT policy for approval by the sponsoring organization prior to this research; with your understanding of the following guidelines in accordance with USAF policy:

a. Take appropriate measures to safeguard all Personally Identifiable Information during the survey;

b. Obtain the express written consent of HQ USAF prior to releasing any material associated with the survey;

c. Properly dispose of any material associated with the survey at the survey conclusion; and

d. Provide a complete copy of the research and all findings to this office at the conclusion of the study.

2. Our AFCESA survey organizational sponsors are Ms. Joanie Campbell or Dr. Daryl Hammond, HQ AFCESA/CEOA, DSN 523-6354/6352, respectively. They look forward to working with Lt Col Jeffrey Humphries and Mr. Juan Lopez on this Delphi Survey.

MAX E. KIRSCHBAUM, Colonel, USAF
Commander

Appendix H: Survey Instrument

Proposed Information Assurance controls for DoD Industrial Control Systems

Primary Investigators: Lt Col J.W. Humphries and Mr. J. Lopez Jr.

Student Researcher: Capt E.A. Mendezllovet

Research Sponsor: HQ USAF A4/7 and AFCESA

Purpose: To seek USAF Civil Engineering SME consensus for proposed Information Assurance controls to address security concerns specific to DoD Industrial Control Systems

Background: The current DoD Information Assurance (IA) controls were last published in 2003 and do not adequately address cyber security aspects unique to Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) systems. This research effort combines recommended best practices from a variety of sources to derive a specific set of IA controls that can be incorporated into the DoD IA control framework. Many ICS or SCADA IA controls map to the DoD framework with no translation required. However, other IA controls were so specific to ICS or SCADA that some interpretation or translation is required. This survey contains the set of ICS or SCADA IA controls:

That require translation to fit into an "existing" DoD IA control subject category

That require interpretation to fit into a "newly created" DoD IA control subject category

The rest of this survey is organized into three parts: (1) Demographics, (2) Ranking of ICS IA control category areas, and (3) Likert scale measurement of proposed new IA controls subject categories. Instructions are provided for part II and III of the survey.

PART I - Demographics:

1. What Major Command are you affiliated with (select only one)?

   a. ACC
   b. AETC
   c. AFGSC
   d. AFMC
   e. AFRC
   f. AFSPC
   g. AFSOC
   h. AMC
   i. PACAF
   j. USAFE
   k. Other: _____________

2. How many years of experience in Control Systems do you have?

   a. Less than one year
   b. 1-3 years
   c. 4-7 years
   d. 8-11 years
   e. Twelve or more years

3. What computer security or network security training have you completed, list all that apply?

   ____

   ____

   ____

4. What certifications have you successfully completed (e.g. Security+), list all that apply?

   ____

   ____

   ____

5. What is your affiliation with the government (Select all that apply)?

   a. Contractor
   b. Military (Reserve, Guard, or Active Duty)
   c. Civil Service employee
   d. Other (Describe) ________________________________

PART II - Rankings:

Instructions: Rank the following ICS security controls in order of importance for the day-to-day operations of USAF control systems. The rankings are grouped by control category area (i.e. three separate grouped rankings). Place importance on the graveness of the impact if the service becomes disrupted or unavailable. Start with "one" being the most important. Note: Email attachment contains control definitions

	Control Area Category (Rankings: 1 - 4)	**Rank**
Management Controls	Risk Assessment (Page 6-2)	
	Planning ((Page 6-3)	
	System and Service Acquisition (Page 6-4)	
	Certification, Accreditation, and Security Assessments (Page 6-5)	
	Control Area Category (Rankings: 1 - 15)	**Rank**
Operational Controls	Personnel Security (Page 6-7)	
	Physical & Environmental Protection, (Page 6-7)	
	Control Center/Control Room (Page 6-10)	
	Portable Devices (Page 6-10)	
	Cabling (Page 6-10)	
	Contingency Planning (Page 6-11)	
	Disaster Recovery Planning (Page 6-12)	
	Configuration Management (Page 6-13)	
	System and Information Integrity (Page 6-14)	
	Malicious Code Detection (Page 6-15)	
	Intrusion Detection and Prevention (Page 6-15)	
	Patch Management (Page 6-16)	
	Media Protection (Page 6-18)	
	Incident Response (Page 6-18)	
	Awareness and Training (Page 6-21)	
	Control Area Category (Rankings: 1 - 11)	**Rank**
Technical Controls	Identification and Authentication (Page 6-22)	
	Password Authentication (Page 6-23)	
	Physical Token Authentication (Page 6-25)	
	Role-Based Access Control (Page 6-27)	
	Web Servers (Page 6-28)	
	Virtual Local Area Network (Page 6-28)	
	Dial-up Modems (Page 6-29)	
	Wireless (Page 6-30)	
	Audit and Accountability (Page 6-31)	
	Encryption (Page 6-33)	
	Virtual Private Network (VPN) (Page 6-34)	

PART III – Agreement Measurements:

Part A:

Instructions: This part contains three ICS IA controls that are not specifically addressed in the DoD IA control framework. Given their relevance and importance in a control systems environment, do you agree that the ICS security topic in column B should be incorporated to the DoD IA control in column A? Using a 5-point scale, indicate your level of agreement with incorporating ICS security control to the DoD IA control. For example, marking 5 indicates that you strongly agree that RBAC in column B fits under ECLP from column A and the verbiage should be added to the definition of the DoD IA control. Marking 1 would indicate that you strongly disagree that RBAC fits into ECLP; therefore it should not be incorporated.

A. DoD IA Control: ECLP **Enclave Computing Environment (EC)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**B. ICS IA** **Access Control**
Least Privilege (LP): Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization	1	2	3	4	5	**6.3.2.1. Role Based Access Control (RBAC):** RBAC can be used to provide a uniform means to manage access to ICS devices while reducing the cost of maintaining individual device access levels and minimizing errors. RBAC should be used to restrict ICS user privileges to only those that are required to perform each person’s job (i.e., configuring each role based on the principle of least privilege).
Additional Comments:						

Q-1

A. DoD IA Control: EBRP **Enclave Boundary Defense (EB)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**B. ICS IA** **Access Control**
Remote Access for Privilege Functions (RP): Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/IAO reviews the log for every remote session.	1	2	3	4	5	6.3.2.4. Dial-up Modem. - Consider using callback systems when dial-up modems are installed in an ICS. This ensures that a dialer is an authorized user by having the modem establish the working connection based on the dialer's information from a callback number stored in the ICS approved authorized user list. - Ensure that default passwords have been changed and strong passwords are in place for each modem. - Physically identify modems in use to the control room operators. - Configure remote control software to use unique user names and passwords, strong authentication, encryption if determined appropriate, and audit logs. Use of this software by remote users should be monitored on an almost real-time frequency. - If feasible, disconnect modems when not in use or consider automating this disconnection process by having modems disconnect after being on for a given amount of time. It should be noted that sometimes modem connections are part of the legal support service agreement with the vendor (e.g., 24x7 support with 15 minute response time). Personnel should be aware that disconnecting/removing the modems may require that contracts be renegotiated.
Additional Comments:						

Q-2

A. DoD IA Control: EBRP **Enclave Boundary Defense (EB)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**B. ICS IA** **Access Control**
Remote Access for Privilege Functions (RP): Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/IAO reviews the log for every remote session.	1	2	3	4	5	**6.3.2.2. Web Servers.** SCADA and historian software vendors typically provide Web servers as a product option so that users outside the control room can access ICS information. In many cases, software components such as ActiveX controls or Java applets must be installed or downloaded onto each client machine accessing the Web server. Some products, such as PLCs and other control devices, are available with embedded Web, FTP, and e-mail servers to make them easier to configure remotely and allow them to generate e-mail notifications and reports when certain conditions occur. When feasible, use HTTPS rather than HTTP, use SFTP or SCP rather than FTP, block inbound FTP and e-mail traffic, etc.
Additional Comments:						

Q-3

Part B

Instructions: This part contains five ICS IA that didn't translate into an existing DoD IA control; additional interpretation is required in order to recommend a "new subcategory area" that will adequately address the ICS security concern. Do you agree that the ICS security topic in column B should fit under newly created DoD IA control in column A? Using a 5-point scale, indicate your level of agreement with creating new DoD IA control to encompass ICS security topic from column B. For example, marking 5 indicates that you strongly agree that Environmental Control Systems in column B fits under PETS from column A. Marking 1 would indicate that you strongly disagree Environmental Control Systems fits into PETS; therefore it should not be incorporated.

A. DoD IA Control: PETS **Physical and Environment (PE)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**B. ICS IA** **Physical and Environmental Protection**
[New DoD Subcategory] **Toxic Substance Controls (TS):** No current definition available///	1	2	3	4	5	**Environmental Control Systems.** Heating, ventilation, and air conditioning (HVAC) systems for control rooms must support plant personnel during normal operation and emergency situations, *which could include the release of toxic substances.* Fire systems must be carefully designed to avoid causing more harm than good (e.g., to avoid mixing water with incompatible products). HVAC and fire systems have significantly increased roles in security that arise from the interdependence of process control and security. For example, fire prevention and HVAC systems that support industrial control computers need to be protected against cyber incidents.
Additional Comments:						

Q-4

A. DoD IA Control: PEBP **Physical and Environment (PE)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**B. ICS IA** **Physical and Environmental Protection**
[New DoD Subcategory] **Blast Protection Controls (BP):** ///No current definition available///	1	2	3	4	5	**Control Center/Control Room.** Providing physical security for the control center/control room is essential to reduce the potential of many threats. In extreme cases, it may be considered necessary to make the control center/control room blast-proof, or to provide an offsite emergency control center/control room so that control can be maintained if the primary control center/control room becomes uninhabitable.
Additional Comments:						

Q-5

A. DoD IA Control: PEAD **Physical and Environment (PE)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**B. ICS IA** **Physical and Environmental Protection**
[New DoD Subcategory] **Access Controls to ICS Devices (AD):** ///No current definition available///	1	2	3	4	5	**Portable Devices.** Computers and computerized devices used for ICS functions (such as PLC programming) should never be allowed to leave the ICS area. Laptops, portable engineering workstations and handhelds (e.g., 375 HART communicator) should be tightly secured and should never be allowed to be used outside the ICS network. Antivirus and patch management should be kept current.
Additional Comments:						

Q-6

A. DoD IA Control: PETP **Physical and Environment (PE)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**B. ICS IA** **Physical and Environmental Protection**
[New DoD Subcategory] **Transmission Medium Protection (TP):** ///No current definition available///	1	2	3	4	5	**Cabling.** Cabling design and implementation for the control network should be addressed in the cyber security plan. Unshielded twisted pair communications cable, while acceptable for the office environment, is generally not suitable for the plant environment due to its susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration. Industrial RJ-45 connectors should be used in place of other types of twisted pair connectors to provide protection against moisture, dust and vibration. Fiber-optic cable and coaxial cable are often better network cabling choices for the control network because they are immune to many of the typical environmental conditions including electrical and radio frequency interference found in an industrial control environment. Cable and connectors should be color-coded and labeled so that the ICS and IT networks are clearly delineated and the potential for an inadvertent cross-connect is reduced. Cable runs should be installed so that access is minimized (i.e., limited to authorized personnel only) and equipment should be installed in locked cabinets with adequate ventilation and air filtration.
Additional Comments:						

Q-7

A. DoD IA Control: DCVP **Security Design and Configuration (DC)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**	**B. ICS IA** **Access Control**
[New DoD Subcategory] **Virtual Partitioning (VP):** ///No current definition available///	1	2	3	4	5	**Virtual LAN (VLAN).** VLANs have been effectively deployed in ICS networks, with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches.
Additional Comments:						

Q-8

Thank you for your participation in this Delphi study. I you need assistance completing the survey responses you can contact Capt Mendezllovet at (813)335-9034 or Mr. Lopez at (937)255-6565 at extension 4637. Please submit your completed responses via email to eddie.mendezllovet@afit.edu located at the Air Force Institute of Technology in Wright Patterson AFB, Ohio.

Appendix I: AFIT IRB Approval

March 1, 2010

Lt Col Humphries,

I have reviewed your study entitled "Information Assurance Controls for DoD Industrial Control Systems" and found that your study qualifies for an IRB exemption.

Per 32 CFR 219.101 (b)(2), Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless: (i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation is exempt.

Your study qualifies for this exemption because the demographic data you are collecting cannot realistically be expected to map a given response to a specific subject, and the questions you are asking could not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation. Finally, while you are collecting names, this is a required and natural consequence of your selected data collection methodology. These names will be protected at all times, only be known to the researchers, and managed according to the AFIT interview protocol.

This determination pertains only to the Federal, DoD, and Air Force regulations that govern the use of human subjects in research. It does not constitute final approval to conduct the study which should be granted by you research advisor. Further, if a subject's future response reasonably places them at risk of criminal or civil liability or is damaging to their financial standing, employability, or reputation, you are required to file an adverse event report with this office immediately.

WILLIAM A. CUNNINGHAM, PhD
AFIT IRB Research Reviewer

Bibliography

Abrams, Marshall (2007); MITRE Technical Report: Addressing ICS in NIST SP 800-53; Retrieve December 2009 from http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/ICS-in-SP800-53_final_21Mar07.pdf

AF 33-200. (2008). *Information Assurance (IA) Management.* Retrieved November 30, 2009 from http://www.e-publishing.af.mil/shared/media/epubs/AFI33-200.pdf

AF 33-210. (2008). *Air Force Certification and Accreditation Program.* Retrieved November 30, 2009 from http://www.e-publishing.af.mil/shared/media/epubs/AFI33-210.pdf

AFI 36-2601. (1996). *Air Force Personnel Survey Program.* Retrieved November 30, 2009 from http://www.e-publishing.af.mil/shared/media/epubs/AFI36-2601.pdf

Engineering Technical Letter (ETL) 09-11, (2009). *Civil Engineering Industrial Control System Information Assurance Compliane.* Air Force Civil Engineer Support Agency. Retrieved Feb 3, 2010 from http://www.wbdg.org/ccb/AF/AFETL/etl_09_11.pdf

Baker, S., Waterman, S., Ivanov, G. (2010). *In the Crossfire: Critical Infrastructure in the Age of Cyber War.* McAfee, Inc. Retrieved Feb 20, 2010 from http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf

Bendel, M. (2006). *An Introduction to Department of Defense IA Certification and Accreditation Process* (DIACAP), Washington, DC: Lunarline, March.

Blyth, A. and G. Kovacich (2006). Information assurance: security in the information environment, Springer-Verlag New York Inc.

Brown, G., M. Carlyle, et al. (2006). *"Defending critical infrastructure."* Interfaces **36**(6): 530-544.

Campbell, P. (2007). The evolving story of information assurance at the DoD, SAND2006-7179, Sandia National Laboratories.

Gibbons, J. D. (1976) *Nonparametric Methods for Quantitative Analysis*, New York: Holt, Rinehart, & Winston, 273-298.

Congressional Budget Office (CBO). (1983). Public Works Infrastructure: Policy considerations for the 1980s. Retrieved 12 Nov 09 from http://www.cbo.gov/doc.cfm?index=5046&type=0

Conover, W. J. (1980) *Practical Nonparametric Statistics 2nd Edition*, New York: John Wiley & Sons, 257-298.

Dacey RF. (2004) Critical infrastructure protection, challenges and efforts to secure control systems. United States general accounting office, GAO-04-354, http://www.gao.gov/new.items/d04354.pdf; 2004[accessed Nov 16, 2009]

Denere, Glenn. (2009). How vulnerable is U.S. infrastructure to a Major Cyber Attack? Popular Mechanics, April 2009 issue. Retrieved Feb 2, 2010 from http://www.popularmechanics.com/technology/military_law/4307521.html

DoD IA C&A Process (DIACAP). (2010). DIACAP Knowledge Service. Retrieved 17 Feb 2010 from https://diacap.iaportal.navy.mil/ks/Pages/default.aspx

DoDI 8500.1, *"Department of Defense Information Assurance,"* Oct 2002

DoDI 8500.2, "*Department of Defense Information Assurance Implementation,"* Feb 2003

DoDI 8510.1, "*Department of Defense Information Assurance Certification and Accreditation Process (DIACAP),"* Nov 2007

DoDI 8580.1, *"Department of Defense Information Assurance in the Defense Acquisition System,"* Jul 2004

Gibbons, J. D. (1976) *Nonparametric Methods for Quantitative Analysis*, New York: Holt, Rinehart, & Winston, 273-298.

Government Accounting Office (GAO), (2004). *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.* Report to Congressional Requesters. 2004. Retrieved 20 Nov 2009 from http://ww.gao.gov/new.items/d04354.pdf

Government Accounting Office (GAO), (2006*). Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics.*
Report to Congressional Requesters. 2006. Retrieved 20 Nov 2009 from http://www.gao.gov/new.items/d0739.pdf

Guttromson, R., A. Schur, et al. (2007). *Human Factors for Situation Assessment in Power Grid Operations,* Technical Report PNNL-16780, Richland, WA.

Hathaway, M, (2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure.* U.S. Cyberpolicy review. Retrieved Feb 2, 2009 from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Hulitt, E. and R. Vaughn Jr (2008). "Information System Security Compliance to FISMA Standard: A Quantitative Measure." Computer Science and Information Technology, 2008. IMCSIT 2008. International Multiconference on: 799-806.

Igure, Vinay. (2008). *Security Assessment of SCADA Protocols: A Taxonomy Based Methodology for the Identification of Security Vulnerability in SCADA Protocols.* VDM Dr. Muller & Co.

Katzke, S., K. Stouffer, et al. (2006). *"Applying NIST SP 800-53 to Industrial Control Systems."* ISO EXPO: 17-19.

Langevin, R., R. McCaul, et al. (2008). *"Securing Cyberspace for the 44 th Presidency."*

Lee, S., Gail-Joon Ahn and Robin A. Gandhi (2005). Engineering information assurance for critical infrastructures: The DITSCAP automation study Retrieved from 10.1.1.108.8998[1].pdf

Lewis, T. (2006). Critical infrastructure protection in homeland security: defending a networked nation, John Wiley and Sons.

Martin, C. (2006). "Protecting America's Critical Infrastructure: Making Our Program More."

Martin, N. (2007). Addressing IT Security for Critical Control Systems. System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Moteff, J. and P. Parfomak (2004). Critical infrastructure and key assets: definition and identification, LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Moteff, J (2008). Critical infrastructure: Background, Policy and Implementation, LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE. Retrieved 12 Nov 2009 from http://www.fas.org/sgp/crs/homesec/RL30153.pdf

Ning, C., W. Jidong, et al. (2008). SCADA system security: Complexity, history and new developments. Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on.

Office of Management and Budget (OMB). (2000). Appendix III to OMB Circular No. A-130: Security of Federal Automated Information Resources. Retrieved 12 Nov 2009 from http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.aspx

Office of the Secretary of Defense (OSD). (2009). Deputy Director of Defense Research & Engineering Deputy Under Secretary of Defense (Science & Technology) Small Business Technology Transfer Research (STTR) Retrieved 12 Nove 2009 from www.acq.osd.mil/osbp/sbir/solicitations/sttr09B/osd09B.doc

Papa, M. and S. Shenoi (2008). Critical Infrastructure Protection II, Springer.

Ralston, P. A. S., J. H. Graham, et al. (2007). "Cyber security risk assessment for SCADA and DCS networks." ISA Transactions **46**(4): 583-594.

Ross, R., S. Katzke, et al. (2005). The new FISMA standards and guidelines changing the dynamic of information security for the federal government. **2:** 864.

Senft, S. and F. Gallegos (2008). Information Technology Control and Audit, Auerbach Publications.

Shaw, William. (2006). Cybersecurity for SCADA Systems. Penwell Corporation.

SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations.* National Institute for Standards and Technology, SP 800-53, August 2009.

SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, National Institute for Standards and Technology, SP 800-82 (draft), August 2008.

Stouffer, K. (2005). "NIST Industrial Control System Security Activities." NIST http://csrc. nist. gov/ispab/2005-09/ISPAB-KStouffer. pdf.

Stouffer, K., J. Falco, et al. (2008). "Guide to industrial control systems (ICS) security." NIST Special Publication **800**: 82.

Tyler Gene (2006); IAnewsletter: IATAC Chat; Vol 9 No 3 pag 3. Retrieved from Http://iac.dtic.mil/iatac

Wiles, J., T. Claypoole, et al. (2008). Techno Security's Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure, Syngress Press.

Willett, K. (2008). Information Assurance Architecture, Auerbach Publications.

Zar, J. H. (1982). Signifcance testing of the Spearman rank correlation. Journal of the Amercan Statistical Association. 67, 578-580.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 25-03-2010	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From – To)* September 2008 – March 2010

4. TITLE AND SUBTITLE Codifying Information Assurance Controls for Department of Defense (DoD) Supervisory Control and Data Acquisition (SCADA) Systems (U)	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Mendezllovet, Eddie A., Captain, USAF	**5d. PROJECT NUMBER** JON 10-360 **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	**8.PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GCO/ENG/10-13
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Civil Engineering Support Agency Attn: Ms. Joanie Campbell 139 Barnes Dr. Suite 1, Tyndall AFB FL 32403-5319 DSN 523-6354, email: Joanie.campbell@tyndall.af.mil	**10.SPONSOR/MONITOR'S ACRONYM(S)** AFCESA/CC **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Protecting DoD critical infrastructure resources and Supervisory Control and Data Acquisition (SCADA) systems from cyber attacks is becoming an increasingly challenging task. DoD Information Assurance controls provide a sound framework to achieve an appropriate level of confidentiality, integrity, and availability. However, these controls have not been updated since 2003 and currently do not adequately address the security of DoD SCADA systems. This research sampled U.S. Air Force Civil Engineering subject matter experts representing 8 Major Commands that manage and operate SCADA systems. They ranked 30 IA controls in three categories, and evaluated eight SCADA specific IA controls for inclusion into the DoD IA control framework. Ranking results (ρ = .972414) indicate a high preference for encryption, and system and information integrity as key IA Controls to mitigate cyber risk. Equally interesting was the perfect agreement among raters on ranking certification and accreditation dead last as an effective IA control. The respondents strongly favored including four new IA controls of the eight considered.

15. SUBJECT TERMS

SCADA, ICS, IA Controls, Supervisory Control and Data Acquisition, Industrial Control Systems

16SECURITY CLASSIFICATION OF:			**17.LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Lt Col Humphries, J.W., PhD, AFIT/ENG
REPORT	**ABSTRACT**	**THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
u	u	u	UU	140	(937) 255-6565, ext 7253 (jeffrey.humphries@afit.edu)

Standard Form 298 (Rev. 8-98)

Prescribed by ANSI Std. Z39-18