The Impact of the New Credential Systems on the Electronic Security Systems

Since September 11, 2001 the United States has been facing additional new challenges to its security among them: cyber threats, natural disasters, health & food threats, economic challenges, and many others. As a result, the White House and Congress continue creating many new directives and initiatives in order to protect the U.S. from these threats. One unique example is The Homeland Security Presidential Directive 12 (HSPD12), which is becoming the genesis for many of the new changes and transformations of our electronic security systems that are protecting our homeland. The HSPD12 Initiative resulted in the PIV card which is a smart card with many physical and logical security features. The PIV card serves as a tool to protect the identity of an individual.

America is a nation of information systems, thus making this credential a unique tool to protect the cyber space and the physical space. Nowadays, the Washington D.C. metropolitan area as well as many other states, municipalities and cities are contemplating using the same model to produce these type of credentials and other nations in Europe are following the same steps.

Background

Mandates and Directives

In response to the times and this imperative need, all Federal Agencies have been impacted by the different directives and mandates that came from the White House. HSPD12, being the most important of these initiatives, is creating a credentialing standard for all agencies; a few states are already implementing these standards as part of the Real ID Act. In addition, The Homeland Security Presidential Directive 5 (HSPD5), The Homeland Security Presidential Directive 8(HSPD8), The Homeland Security Presidential directive 20, (IPV6), and Energy Efficiency are other mandates that already are paving the way for traditional security systems which will require modernization to meet these compliances.

Homeland Security Presidential Directive 12 (HSPD12)

In the wake of Sept. 11, 2001, the White House staked out a defensive line against terrorist attacks, espionage and cyber threats with its Homeland Security Presidential Directive 12 (HSPD-12). This initiative began the process to create an inter-operable credentialing system for all Executive Branches and agencies of the Federal Government. In addition, the Department of Commerce was tasked with the development of the technical specifications and plans. Under the mandate of the White House, The U.S. National Institute of Standards and Technologies (NIST) developed the Federal Information Processing Standard 201-1 (FIPS201-1). This technical specification and its other associated technical documents (SP 800-73, SP 800-76, SP 800-116, etc.) provide full support and guidance to the HSPD-12 mandate. The Federal Information Publication Standard (FIPS201-1) technical specifications relate only to the guidance and development of the inter-operable Federal Government Credential Card. This card is known to all as the PIV Credential Card. FIPS201-1 also addresses the technical guidance for Card Readers, Card Management, Public Key Infrastructure (PKI), Private Key Infrastructure,

Biometrics and Verification Systems. The Government Standards FIPS201 refer to the use of contact smart cards, contact smart card readers, printers, cameras, biometrics, PKI, certificates, and software associated with the production of interoperable government wide credentialing system. This mandate will accomplish a government-wide interoperable common ID and will eliminate the existing credential systems known as Photo ID Systems in the physical security systems.

Under the leadership of the Interagency Advisory Board (IAB) the federal government agencies produced several documents and user guides that can be found at: www.idmanagement.gov. The IAB is also working in partnership with industry experts such as the Smart Card Alliance, the Security Industry Association and Condortech Services, Inc. along other institutions and Companies. NIST has also developed and implemented the new Standard Publication 800-116 (SP 800-116); this standard publication has been released and specifically relates to the Physical Access Control implementation.

Since the IAB' creation, Condortech Services, Inc. and its staff supported and joined this initiative and took into consideration the importance of HSPD12 including full compliance with the HSPD12 goals and objectives.

Homeland Security Presidential Directive 20 (HSPD20)

This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. In addition, this policy establishes: a) "National Essential Functions;" b) prescribes continuity requirements for all executive departments and agencies; and c) provides guidance for State, local, territorial, tribal governments, and private sector organizations. All these requirements necessary to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

"Continuity of Operations," or "COOP," means an effort within individual executive departments and agencies to ensure that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

Electronic Security Systems are vital tools for the effective implementation of these types of directives, and depending on the electronic system's configuration, they can become a valuable pillar to support the spirit of this directive.

Cyber Security Act of 2009

(S.773) was introduced in Congress to provide legislation to ensure the continued free flow of commerce within the United States as well as with its global trading partners through secure cyber communications. In this regard, it contributes to the continuous development and exploitation of the Internet and intranet communications, provides for the development of a cadre of information technology specialists to improve and maintain effective Cyber security defenses against disruption, and for other purposes.

Electronic Security Systems

Electronic Security Systems have been providing services to control access, surveillance and detection of threats all within the limits of the hardware installed. Most physical security systems are composed of Smart Card Readers, RFID Readers, IP Cameras, Analog Cameras, Digital Recorders, Network Video Recorders, Net-workable Controllers, IP Wireless Devises, Servers and different other peripherals. There are also many electro-mechanical devices that are connected for its activation or deactivation through means of its controllers, in which gates, doors, etc. will open or close or even detect intrusion or provide video or audio; all depending on how they are physically configured. These systems and peripherals are integrated into a command and control center to provide information, audio, video, and data to the security staff. Some of the most modern systems have been upgraded to automate its processes and operation to include technology automation mostly, by adding software layers on top of the existing security applications. Typically these systems are proprietary and have been interconnected between their own networks. In essence, Electronic Security Systems are more heavily dependent on hardware than software. Software is typically used for collecting and displaying data, information, video, control inputs and outputs.

In addition to the latest mandates and directives, the security systems to be installed at Federal government agencies must be in compliance with local electrical codes, UL certifications, life safety, and other regulations depending on the territory where the installation takes place.

Overall, these security systems have their own challenges due to regulations, directives and training. They are complex in nature and they are free from becoming targets of viruses, Trojans, etc. or any type of cyber attacks, since their environments are closed.

Security Convergence Initiatives

A number of initiatives have been created by the security industry as well as other interest groups with initiatives to utilize existing network infrastructure from the Agency's CIO, thus interconnecting logical and physical security systems in order to make processes for the use of the PIV card much more effective. This is in part justified, since the Physical and Logical security staff, both tasked with protecting enterprise assets, are seeing increased technology and budgetary overlaps. In addition, technological shifts, budgetary realities and major government initiatives are adding further impetus for convergence of these two factions.

Physical and logical security staffs have the same goals and that is to protect enterprise assets. Yet, they exist as independent factions, since their systems are not interconnected. There are also cultural barriers to consider and it is not always a peaceful process. However, technological shifts, budgetary realities and major government initiatives are doing some converging of their own and driving enterprises to question whether business as usual is actually hurting the bottom line.

In order to achieve these goals, both systems will have to share the same network infrastructure and depend more on LAN or WAN networks, servers and digital storage mediums.

The positives about converge is that physical security systems can now have redundancies of operations among their systems and have the ability to operate virtually the command and control centers from a single point or multiple remote sites. In the past, the Redundancy of Command and control Centers could not have been achieved effectively due to the limitation of their local networks. Today, these

Command and Control Centers have the ability to become a very effective tool of moving data, video and/or audio during natural disasters or any other types of events.

Physical security professionals find this trend a cause for concern and with good reason, since most of those systems do not have the necessary protections for Cyber attacks once these systems are on the networks.

Cyber Security

By now, we all know that in this Information Age the most modern warfare would be attacking the US information infrastructure systems, which are composed of millions of servers, computers interconnected via the internet. Millions of people depend on these information systems to either make a bank transaction or a purchase of an item or secure their facilities. Most recently for instance, we have witnessed how effective the Iranian opposition was in delivering data and video by disrupting their government information security systems, even while their government had made strong efforts to control the information flow of their systems. The Electronic Security Systems are also vulnerable to these types of attacks, through either viruses or any other type of electronic warfare, which may impact the operation of the system. Some Government agencies are now using IP cameras as part of their Intelligent Transportation Systems. Some other agencies are also using IP controllers that are now part of this type of environment due to the convergence initiatives.

The Challenge

Since most of the electronic security systems use micro-controllers, servers, workstations, IP cameras, IP sensors, etc. they will be or are already connected to the CIO's networks. Unfortunately, these systems lack on the ability to be authenticated through any other means other than a password or a handshake through an algorithm from its software security application. Passwords needed to open up any of those devices, i.e. micro-controllers sent via hardwired network and opened to be intercepted. Most of them lack network administration or are not tied to active directory. Communication bandwidth is typically via RS232 connected with the use of an interface that converts its data to an IP communication. Micro-controllers do not have sufficient speed or memory for handling data encryption. Most cameras are being built with TCP/IP connectivity and do not yet meet the IPV6 compliance, nor can they be authenticated through a certificate or another form of security to protect them from cyber attacks. There have been major investments on electronic security legacy systems that now will need to be migrated. Interoperability is a key component to minimize these future expenses. It will cost more in the long run if components of the legacy systems are upgraded in order to meet just certain directives, like in the case of HSPD12. There are other directives and regulations that are related to HSPD12, and they will have a major impact in implementing them into the electronic security system later on.

When NIST developed the HPSD12 technical documents, NIST had only focused on the issuance of cards, therefore processes and specification (FIPS201-1, SP800-73, etc.) were developed for biometric readers, card readers, smart card, printer or any other peripheral to implement a new credential (PIV Card). However, the rest of the other systems such as controllers, security software, peripherals, etc. were not specified in any of those technical documents from NIST. The use of the new credential is forcing Physical Security Access Control System (PACS) to ride on the networks and yet some of those controller or interfaces are not encrypted. The database on most of these systems is also not encrypted, nor do they meet some of the NIST standards like FIPS 140-2.

The Solution

Education and awareness is a key factor to mitigate these challenges, and although typically there are cultural barriers between Physical Security and IT Security professionals, both groups have something in common, which is protection, deterrence, monitoring and surveillance. of the physical and virtual assets of the Government Agency.

The migration and implementation plan of these systems will need to include all directives and initiatives that are impacting the electronic security systems and at the same time, integrate current legacy regulations and codes. In addition, technical specifications will require to include parameters and technical criteria from the physical security, logical security and cyber security technologies.

In summary, the Federal Government has many security initiatives and directives in place, and technology will need to be driven by these directives. Moreover, technology will need to be compliant with a concentration on being "directive-centric" rather than "technology–centric".

9/1/2009

X 

Jorge G. Lozano
CEO/President

Condortech Services, Inc.
3700 Wheeler Ave.
Alexandria, VA 22304
P: (703)-916-9200
F: (703)-642-5184
www.condortech.com