



Information Assurance, DIACAP Compliance, and Video Security

By Danny Graves, Information Assurance Team Leader





Introduction

The migration of video security from traditional closed analog hardware systems to networked systems running on open standards-based IT architectures brings new challenges and opportunities. The integration of digital video security solutions into existing IT infrastructures is very attractive for distributors, integrators and end users – reducing cost and time of installation, improving ease of use and management, while enhancing system capabilities through converged security architecture and technology. At the same time, manufacturers of video security systems must ensure their digital solutions do not introduce potential security risks to IT infrastructures and/or create risk management issues for organizational leadership. Specifically, there is a need for video security systems that are designed to support and comply with increasingly stringent security standards for automated information systems (AIS) in key segments of the market, including government and financial institutions.

Video Security and Automated Information Systems

Video security presents a challenge in an era of greater concern about network security, because digital video security products have tended to differ from “traditional network devices”, especially when it comes to information assurance. Although digital video security products, such as digital video recorders (DVRs) are designed using open systems standards and are interoperable with other equipment, these devices typically are not easily managed, configured or upgraded by on-site security engineers or administrators. This fact has prevented local administrators from implementing vulnerability remediation on many digital video security products without serious impact to the products’ availability and integrity.

Information Assurance

In response to growing awareness and concern about the potential for threats to network security, certain sectors of the video security and surveillance market are adopting new and more stringent standards for network-based automated information systems. A central component of modern approaches to network security is the concept of Information Assurance.

Information assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.¹

The following excerpts are the most commonly referenced definitions for information assurance and provide insight into the different sector perspectives.

Commercial Industry

An engineering discipline that provides a comprehensive and systematic approach to ensuring that individual automated systems and dynamic combinations of automated systems interact and provide their intended functionality, no more and no less safely, reliably and securely in the intended operational environments.²

¹http://en.wikipedia.org/wiki/Information_assurance

²(*ISC² Common Body of Knowledge*)

Federal Government:

Information operations that protect and defend information and information systems by ensuring their Availability, Integrity, Accountability, Confidentiality, and Non-repudiation; including providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.³



Information Assurance Life Cycle

Sector Perspectives

Traditionally the Federal Government has taken a more aggressive approach to protecting information through the creation of security standards and the implementation of policy and controls within its Automated Information Systems. Government Information Assurance is driven by the need to protect resources that are vital to our National Security including the lives of human beings. Penalties for non-compliance begin with loss of connectivity and end with fines and imprisonment.

Commercial industry is more often risk-focused and driven by potential business impact. Industry tends to be less aggressive, often reactive. The exception are those organizations that fall into the highly regulated industries, like banking and health care, and are required to comply with numerous regulations mandated by the Federal State and Local Government and can have serious impact on business if not in compliance. Non-compliance can also lead to jail time, under HIPPA, SOX, and other regulations (see below).

Compliance: Industry

The foundation of any information assurance program begins with the Information Assurance framework. Simply put, the strategy is often “begin with the end in mind.” What level and type of compliance or accreditation are we subject to or are we trying to achieve? In industry, this may entail international standards like ISO, or PCI, payment card industry compliance. Within the government sector, the focus is certification and accreditation and is most often based on the Federal Information Security Management Act (FISMA) or the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). Within industry, there are many compliance frameworks, the following is a list of most common compliance

³(DODD S-3600. 1 Information Operations)

frameworks defined and regulated through US Government laws, Acts or Regulations, U.S. and international standards, organizational bylaws and best practices publications.

Financial

(PCI-DSS Compliance) Payment Card Industries – Data Security Standard

The PCI-DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

(SOX Compliance) Sarbanes-Oxley Act

The Sarbanes-Oxley Act establishes a set of requirements for financial systems, to deter fraud and increase corporate accountability. For information technology systems, regulators may need to know who used a system, when they logged in and out, what accesses or modifications were made to what files, and what authorizations were in effect. IT vendors responding to Sarbanes-Oxley requirements have adopted Role-Based Access Control (RBAC) as central to compliance solutions, because RBAC was designed to solve this type of problem.

(GLBA Compliance) Gramm-Leach-Bliley Act

Section 501 of the Gramm-Leach-Bliley Act (GLBA) documents specific regulations required for financial institutions to protect “non-public personal information”. As part of the GLBA requirements, it is necessary that a security management process exists in order to protect against attempted or successful unauthorized access, use, disclosure, modification, or interference of customer records. In other words being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive customer information.

Health Care

(HIPAA Compliance)- Health Insurance Portability and Accountability Act

The Health Insurance portability and Accountability Act (HIPAA) of 1996 passed to provide insurance portability, fraud enforcement, and administrative simplification for the healthcare industry. The act provides some explicit requirements for documentation retention and Best Practices including very specific and stringent guidelines that include Administrative Safeguard, Physical Safeguard, and Technical Safeguards.

International Standards

International Organization for Standardization 27002 (17999)

The ISO 17779 establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.

Compliance: US Government Accreditation

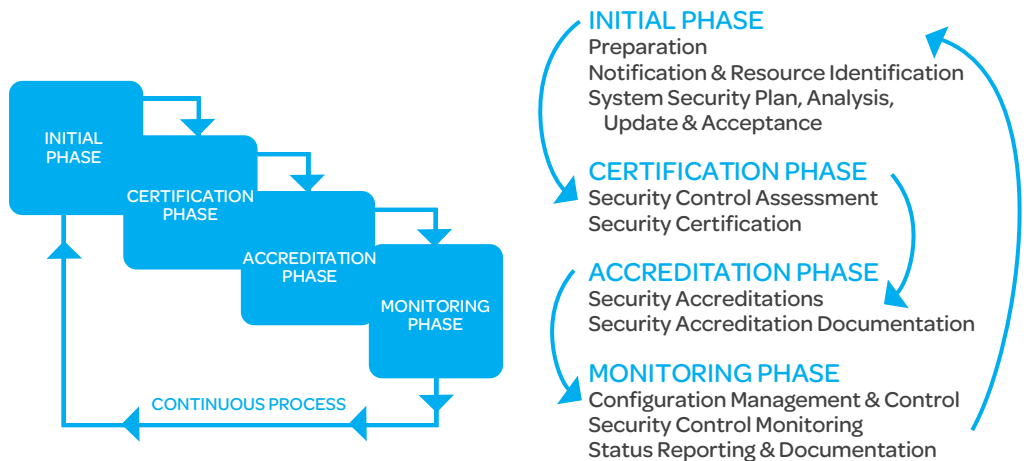
The U.S. Government Accreditation process involves certifying and accrediting a whole system in a particular environment. Certification and accreditation defined as follows⁴:

Certification

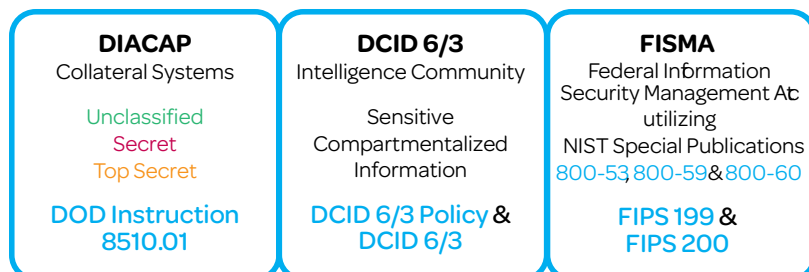
A comprehensive analysis of the technical and non-technical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. *Note: Certification is accomplished in support of the accreditation process and targets a specific environment.*

Accreditation

A formal declaration by a Designated Approving Authority (DAA) that an AIS is approved to operate (ATO) in a particular security mode using a prescribed set of safeguards. *Note: Accreditation is the formal declaration by a DAA that a system is approved to operate:* (a) in a particular security mode; (b) with a prescribed set of countermeasures (e.g., administrative, physical, personnel, COMSEC, emissions, and computer security controls); (c) against a defined threat and with stated vulnerabilities and countermeasures; (d) within a given operational concept and environment; (e) with stated interconnections to other systems; (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility; and (g) for a specified period.



All Government organizations participate in the Certification & Accreditation process and use different approaches depending on the type of systems that are being accredited:



⁴[NST92]National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, National Information Systems Security (INFOSEC) Glossary, June 1992.

Pelco Approach

Pelco has set the goal of establishing itself as the industry leader in providing security-enabled products for highly regulated markets. To meet this goal, Pelco maintains an Information Assurance compliance team. The Pelco IA team focuses its efforts on Information Assurance within the Pelco integrated IP product line, to establish secure digital video solutions that meet or exceed government, industry and international Information Systems Security Compliance Standards.

Almost every AIS security standard is based upon the Security Guidelines that the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) co-wrote and have maintained since the passage of the Computer Security Act of 1987. Pelco looks to these standards as the baseline security implementation for its product line. Information Assurance is the foundation of a compliance process, which ensures the protection of customer information and data by implementing security best practices within every product that Pelco sells. This process integrates into the software development and engineering life cycles continuously enhancing security from the concept design to end of life.

Pelco is implementing compliance standards based on NIST and ISO “Security Best Practices” into its current product line, while implementing secure development practices into applications and operating systems for future releases. The Pelco approach to information assurance is intended to create a plug-and-play environment for customers who require more stringent information security standards.

In October 2009, Pelco provided a DX8100 version 2.0 HVR to a DOD-sponsored test facility for DIACAP Compliance testing. As a result of that test effort, an Authority to Operate (ATO), good for three years, was provided for the ultimate system, which included deployment of the DX8100.

In addition to DIACAP compliance for DX8100 version 2.0, Pelco is currently working with various government agencies for compliance of Endura, its enterprise video management solution, as well as its IP imaging solutions, including the Sarix line of HD cameras.

Summary

Video security systems pose potential risks for IT installations that are required to comply with strict standards for information assurance. Understanding the special security demands for automated information systems (AIS) in key segments of the market, Pelco is delivering video security solutions that meet the certification and accreditation requirements under DIACAP.



by **Schneider** Electric

The recognized worldwide leader in video and security systems, Pelco boasts the most comprehensive array of products, services and expertise available in today's marketplace. And now as a member of the Schneider Electric family, Pelco brings a network of assets backed by the strength of a Fortune 500 company to help you define and achieve your business objectives.